advidia

VP-4

USER MANUAL

Version1.2.0

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC.

2002/96/EC (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Description on Laser Specification

The optical disc drive such as DVD Super Multi (Double Layer) Drive 22X that is used in this computer is equipped with laser. The classification label with the following sentence is affixed to the surface of the drive.

CLASS 1 LASER
PRODUCT TO IEC60825-1
LASER KLASSE 1

The drive with the above label is certified by the manufacturer that the drive complies with the requirement for laser product on the date of manufacturing pursuant to article 21 of Code of Federal Regulations by the United States of America, Department of Health & Human Services, Food and Drug Administration.

In other countries, the drive is certified to comply with the requirement pursuant to IEC 60825-1 and EN 60825-1 on class 1 laser product.

This computer is equipped with the optical disc drive in the following list according to the model.

Safety Warnings and Cautions

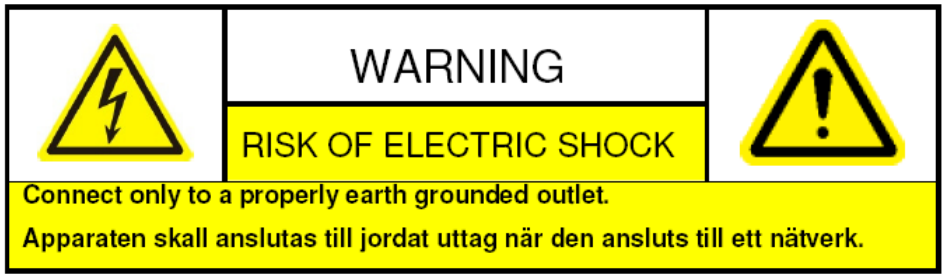
Please pay attention to the following warnings and cautions:

Hazardous Voltage may be present: Special measures and precautions must be taken when using this device. Some potentials (voltages) on the device may present a hazard to the user. This device should only be used by employees from our company with knowledge and training in working with these types of devices that contain live circuits.

Caution
The power supply in this product contains no user-serviceable parts. Refer servicing only to qualified personel.

Power Supply Hazardous Voltage: AC mains voltages are present within the power supply assembly. This device must be connected to a UL approved, completely enclosed power supply, of the proper rated voltage and current.

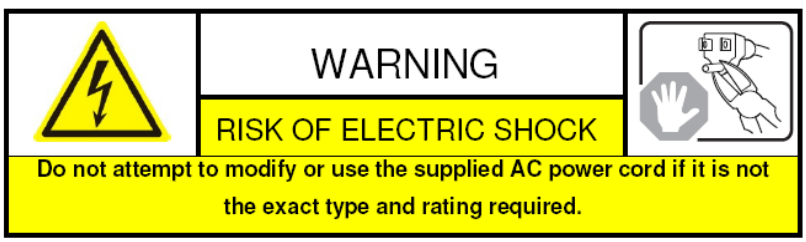
No user serviceable parts inside the power supply.


WARNING
RISK OF ELECTRIC SHOCK
Connect only to a properly earth grounded outlet.
Apparaten skall anslutas till jordat uttag när den ansluts till ett nätverk.

System Grounding (Earthing): To avoid shock, ensure that all AC wiring is not exposed and that the earth grounding is maintained. Ensure that any equipment to which this device will be attached is also connected to properly wired grounded receptacles and are approved medical devices.

Power Connect and Disconnect: The AC power supply cord is the main disconnect device to mains (AC power).The socket outlet shall be installed near the equipment and shall be readily accessible.

Installation and Maintenance: Do not connect/disconnect any cables to or perform installation/maintenance on this device during an electrical storm.


WARNING
RISK OF ELECTRIC SHOCK
Do not attempt to modify or use the supplied AC power cord if it is not the exact type and rating required.

Power Cord Requirements: The connector that plugs into the wall outlet must be a grounding-type male plug designed for use in your region. It must have certification marks showing certification by an agency in your region. The connector that plugs into the AC receptacle on the power supply must be an IEC 320, sheet C13, female connector. See the following website for more information http://kropla.com/electric2.htm.

Lithium Battery: This device contains a Lithium Battery. There is a risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the vendor's instructions and in accordance with local environmental regulations.

Perchlorate Material: Special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate. This notice is required by California Code of Regulations, Title 22, Division 4.5, Chapter 33: Best Management Practices for Perchlorate Materials. This device includes a battery which contains perchlorate material.

Chapter 1 Introduction

1.1 Description

Developed on the basis of the latest encoding technology, the VP-4 allows the analog signal to be digitized and then stored in hard disk or transmitted via network.

Adopting the latest embedded processor, the VP-4 provides more powerful capabilities in audio/video encoding; standard 1U chassis design maintains easy installation; multiple network transmission protocols supported; and code downloaded in FLASH ensures high stability and reliability of system performance.

1.2 Features

Encoding

Support H.264 encoding standard at PS and RTP customized encapsulation formats, of which RTP stream is used for transmission via network and PS stream for recording;

Support encoding at 4CIF, 2CIF, CIF and QCIF resolutions;

Dual stream encoding;

Either compound streams encoding or video stream encoding selectable; audio and video synchronization during compound streams encoding.

Recording

- **Multiple Recording Periods Configurable**

Up to 8 recording periods can be configured for each day, with different recording type selectable for each recording period.

- **Cycle Recording**

Either cycle recording or non-cycle recording mode is configurable. In cycle recording mode, the earliest recoding will be overwritten when the HDD is full; and in non-cycle recording mode, the system will stop recording and give alert when HDD is full.

- **Scheduled & Event Recording**

Each channel can be set with the scheduled recording and event recording separately, with separate resolution, bit rate, frame rate and stream type configurable.

- **Multiple Record Triggering Modes**

Scheduled recording;
Motion detection recording;
Alarm recording;
Motion detection/alarm recording;
Motion detection & alarm recording;
Manual recording.

- **Pre-recoding and Post-recording**

Support pre-recoding and post-recoding, with the recording time configurable: 0-30sec for pre-recording and 5-600sec for post-recording;

- **Record Files Lock & Unlock**

User may lock/unlock the record files, and the locked record files will not be overwritten in cycle-recording mode.

- **HDD Group Management**
- **HDD Property Settings**

The HDD can be set to read/write, read-only or redundancy properties;
When the HDD is set to read-only, it allows search and playback of record files only, and no data can be written into the disk, including record and log;
When the HDD is set to redundancy, it must be used with the read/write disk for real-time backup of important record data.

Network

- One 10M/100Mbps self-adaptive UTP Ethernet interface;
- IPv6 is supported.
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported.
- TCP and UDP for unicast.
- Automatically get IP address by DHCP protocol;
- Two-way audio and single-directional broadcasting;
- Transmission via RS-232 and RS-485 transparent channels;
- Access to Internet by PPPoE method, and support Peanut Hull, Dyndns, NO-IP, etc.;
- Set time by NTP;
- Remote Web browser access by HTTP protocol;
- Connectable with network HDD in NAS, IPSAN mode;
- Send E-mail by SMTP protocol, and support attachment of captured JPEG image and SSL encryption;
- Remote JPEG image capturing with user-defined image resolution and quality.

PTZ Control

- **Support Multiple PTZ Protocols**

Different channels can be configured with protocol type, RS-485 address, baud rate, data bit, stop bit, even & odd parity, stream control method, etc.; and remote configuration of presets, patrols and patterns.

- **Digital Zoom (with Speed Dome)**

When connected with speed dome, digital zooming can be realized by clicking on the image through client software.

- **PTZ linkage**

Relay input alarm can be responded with PTZ linkage actions, e.g., callup of predefined presets, patrols or patterns.

Alarm

- **Relay Alarm Input**

Either NO mode or NC mode can be set;

Four different alarm arming periods are configurable;

Capabilities of triggering corresponding alarm handling methods, relay alarm output, buzzer alarm, upload to control center, PTZ linkage, presets/patrols/patterns callup, etc.

- **Relay Alarm Output**

Relay alarm output can be connected with alarm devices for alarm handling within arming period.

Exceptions

- **Exception Alarm Handling**

Exception alarms include network disconnect alarm, IP address conflict alarm, illegal access alarm, etc.; multiple alarm handling methods are supported, relay alarm output, buzzer alarm, upload to center, etc.

- **Exception Reboot**

Software watchdog capability: for inspecting important tasks and system resources of device; in case of exceptions detected, the device will be automatically rebooted.

Firmware watchdog: for inspecting the firmware of device; in case of exceptions in system task scheduling, the device will be automatically rebooted.

User Administration

A maximum of 32 users can be created by the system, including 1 administrator and 31 users. The user name of the administrator is *admin*, which cannot be modified, and the password is allowable to be modified by the administrator only; no deletion of the administrator is allowed, and the administrator is authorized to set the operation permissions for normal users.

Logs

The system logs can be classified into the operation logs, alarm logs, exception logs and information logs. User may search and view all recorded system logs by date or type, as well as export the logs to the text format over network.

Chapter 2 Structure

2.1 Front Panel

VP-4:

Figure 2.1 Front Panel of VP-4

Table 2.1 Front Panel of VP-4

LED Indicator	Function
POWER	Power LED indicator: 1. Lights in red when the device is working; 2. Does not light when the device is powered off.
LINK	LINK LED indicator: 1. Normally lights in green when the network connection is functioning properly; 2. Does not light when the network connection is abnormal.
Tx/Rx	Tx/Rx LED indicator: 1. Does not light when the network is not connected; 2. Blinks in green when the data is transmitting / receiving; 3. Blinks at higher frequency when the data for transmitting / receiving is larger.

2.2 Rear Panel

VP-4HCI / HFI:

Figure 2.2 Rear Panel of VP-4

Table 2.2 Rear Panel of VP-4

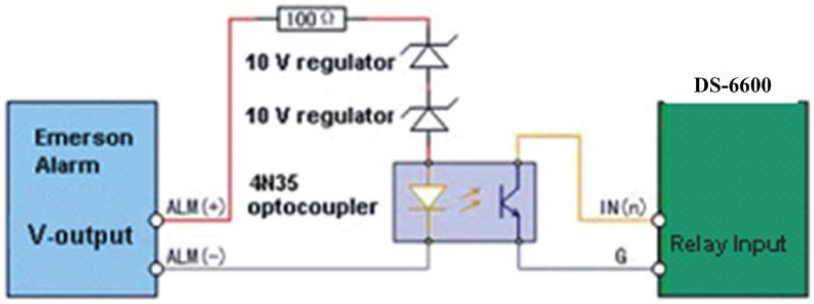
	Interface	Connections
1	GND	Grounding
2	DC12V	12V DC power supply
3	RS-485	RS-485 serial interface for connection to pan/tilt unit, speed dome, etc.
4	ALARM OUT	Relay alarm output.
5	ALARM IN	Relay alarm input.
6	RESET	Restore the factory default settings by holding the *RESET* button for 15 seconds after power is turned on.
7	LAN	10M/100Mbps self-adaptive UTP Ethernet interface.
8	RS-232	Serial interface for configuration of device's parameters or used as transparent channel.
9	VIDEO IN	BNC connectors for video input.
10	AUDIO IN	BNC connectors for audio input.
11	LINE IN	3.5mm two-way audio input interface for connection to active pick-up, microphone, etc.
12	AUDIO OUT	3.5mm audio output interface for connection to audio output device, e.g., loudspeaker, etc.

2.3 Alarm Connections

2.3.1 Alarm Input Connections

VP-4 supports the open/close relay input as the alarm input mode. For the alarm input signal not in open/close relay signal mode, please follow the connections shown as below:

Alarm input connections for Emerson Alarm:



Note: the corresponding relay input port of DS-6600 should be set to NC mode.

Figure 2.3 Alarm Input Connections for Emerson Alarm

Alarm input connections for Normal Alarm:

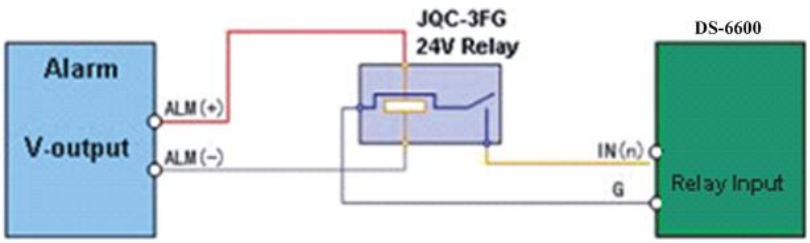
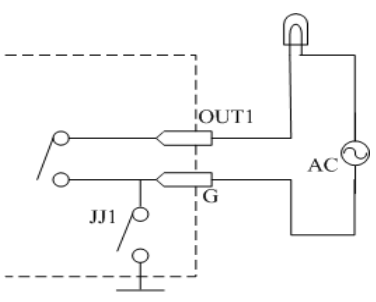


Figure 2.4 Alarm Input Connections for Normal Alarm

2.3.2 Alarm Output Connections

VP-4 supports the open/close relay input as the alarm output mode. The alarm input can be selected to *NO* or *NC*. Different alarm output connection methods are applied to the AC or DC load. Please refer to the following diagram:

Alarm output connections diagram:



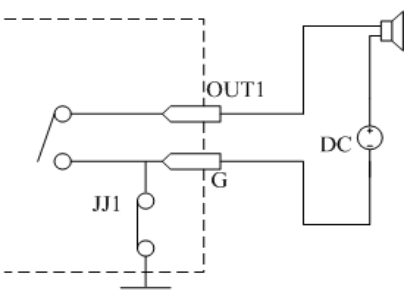


Figure 2.5 Alarm Output Connections

Please note the different connections of JJ1 shown above.

For DC load, JJ1can be safely used both in *NC* and *NO* methods, and it is recommended to use within the limit of 12V/1A. For external AC input, JJ1 must be open. The motherboard provides two jumpers, each corresponding to one alarm output. And both of two jumpers are factory set to be connected.

Chapter 3 Network Parameters Configuration

Purpose:

If you don't know the IP address of the encoder and this is not the first time you use the encoder, you can use Advidia Device Utility or the Serial port tools to find out the IP address of the encoder and to configure the IP address or other network parameters of it. It is recommended to change the default IP address for the first time to use it.

This chapter aims to tell the procedures of using the Advidia Camera Finder software and the Hyper Terminal Software to find and configure the IP address and other parameters of the device.

Note:

For the first-time user, the default user name of VP-4 is *admin*, and password is *12345*. And the default IP address is *192.0.0.64*.

3.1 Hyper Terminal Setup

The common method is to connect encoder and PC with serial line, run Hyper Terminal and modify parameters with serial command. Please connect the RS-232 port of encoder with the COM port of PC directly, power on the encoder and PC and follow the steps:

Step 1: Enter Hyper Terminal.

Click "Start"-> "Programs"->"Accessories"-> "Communications"->"Hyper Terminal" in Windows system, and the dialogue box below will appear:

Figure 3.1 Create New Connections

Step 2: Name the connection and define the icon.

Input a name (e.g. HK), select an icon, and press "OK" to enter "Connect To" dialogue box.

Step 3: Select the communication port.

Select “COM1” in “Connect To” interface (Please select the COM port according to the reality, in case PC has more than 1 COM.). Press “OK” to enter “Properties” dialogue box.

Figure 3.2 Select Communication Port

Step 4: Serial port setup.

Set port parameters in “COM1 Properties” dialogue box as follow:

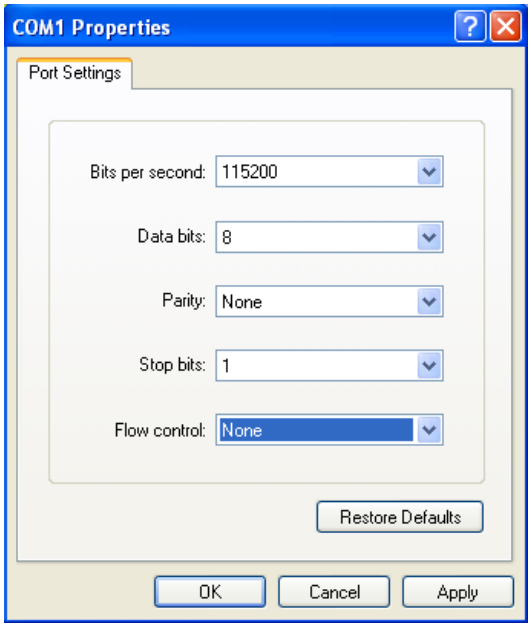


Figure 3.3 Set up Port

The parameters should be:

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Press “Apply” and “OK” after the setup.

Press “Enter” under Hyper Terminal interface. When “$” appears, the connection is established.

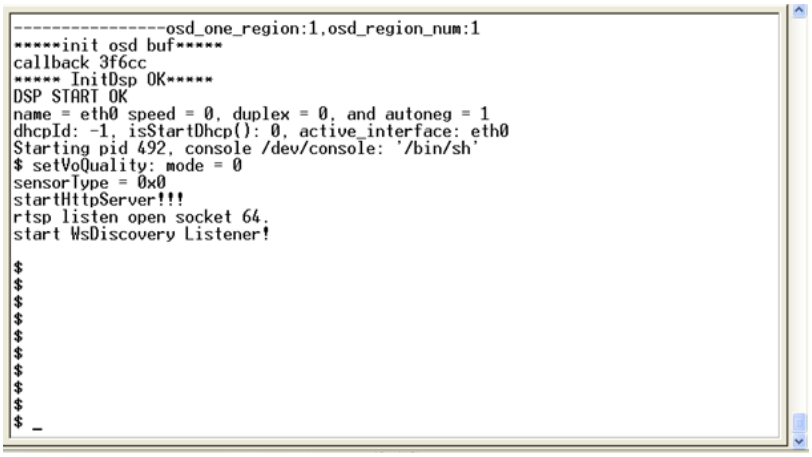


Figure 3.4 Test the Establishment of Connection

Step 5: Disconnect and save connection

According to the tips, disconnect and save “HK” for the next time. After saving, there will be a new “Hyper Terminal” item established in the program group “Start”-> “Accessories”->“Communications”->“Hyper Terminal”. “Connection” names of all Hyper Terminal are included. You can see an icon named as “HK” here.

Figure 3.5 Disconnect and Save Connection

3.2 Network Configuration by Hyper Terminal

Enter Hyper Terminal

Steps:

1. Click “Start”->“Programs”->“Accessories”->“Communications”->“Hyper Terminal”->“HK”, then the Hyper Terminal interface will appear.
2. Press “Enter” and the symbol “$” will appear which means the current default login user is *guest* (please refer to Table 3.1 for the permission of *guest* user account).

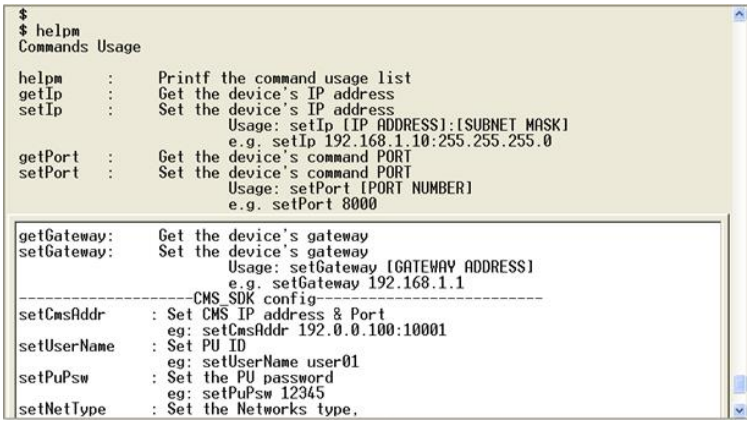

$
$ helpm
Commands Usage
helpm : Printf the command usage list
getIp : Get the device's IP address
setIp : Set the device's IP address
Usage: setIp [IP ADDRESS]:[SUBNET MASK]
e.g. setIp 192.168.1.10:255.255.255.0
getPort : Get the device's command PORT
setPort : Set the device's command PORT
Usage: setPort [PORT NUMBER]
e.g. setPort 8000
getGateway: Get the device's gateway
setGateway: Set the device's gateway
Usage: setGateway [GATEWAY ADDRESS]
e.g. setGateway 192.168.1.1
----------CMS_SDK config----------
setCmsAddr : Set CMS IP address & Port
eg: setCmsAddr 192.0.0.100:10001
setUserName : Set PU ID
eg: setUserName user01
setPuPsw : Set the PU password
eg: setPuPsw 12345
setNetType : Set the Networks type,

Figure 3.6 Enter *guest* User Account

3. Enter *admin* user account.
   (1) Type “su admin” and press “Enter”.
   (2) Input the password (default: 12345) of the *admin* user account.
   (3) Press “Enter” to have the symbol “#”on the interface which indicates the current login user is *admin*.

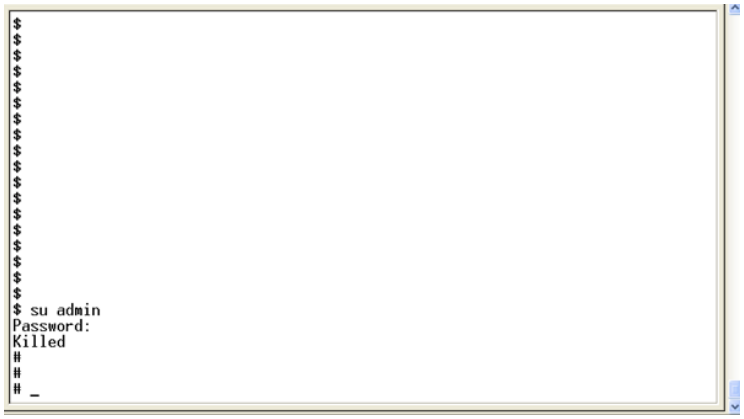


Figure 3.7 Enter *admin* User Account

4. Type the commands described in Table 3.1 to configure the parameters of the device.

Table 3.1 Description of Commands

The *admin* and *guest* have different permission to use commands. Please refer to the following table:

Command	guest	admin	Description
helpm	√	√	Console help command is used to print common commands
getIp	√	√	Get the current IP address of the device. Command format: *getIp* + “Enter”.
setIp	×	√	Set IP address. Command format: *setIp* IP: mask, e.g., *setIp 192..168.1.11:255.255.255.0*
getPort	√	√	Get data port of the current video server. Command format: *getPort*+ “Enter”.
setPort	×	√	Get data port of the video server. Default port: 8000,

			command format: *getPort*+Port No., e.g., *setPort 9000*.
getGateway	√	√	Get current gateway address. Command format: *getGateway*+ “Enter”.
setGateway	×	√	Set gateway. Command format: *setGateway* Gateway, e.g., setGateway 192.168.1.1.
setEnaAlarmSms	×	√	Enable SMS alarm.
setWhiteList	×	√	Set whitelist.
getWhiteList	√	√	Get whitelist.
delWhiteList	×	√	Delete whitelist.
setOffLineTime	×	√	Set offline time.
setCmsAddr	×	√	Set IP address of push mode.
setUserName	×	√	Set user name of push mode.
setPuPsw	×	√	Set password of push mode.
setNetType	×	√	Set network type.
showPuParam	√	√	Get push mode parameters.
setSdkPrint	×	√	Set push mode print.

If you want to switch to *guest* from *admin*, you may type the “su guest” command. When symbol “$” appears, it indicates the current user account has switched to *guest*.

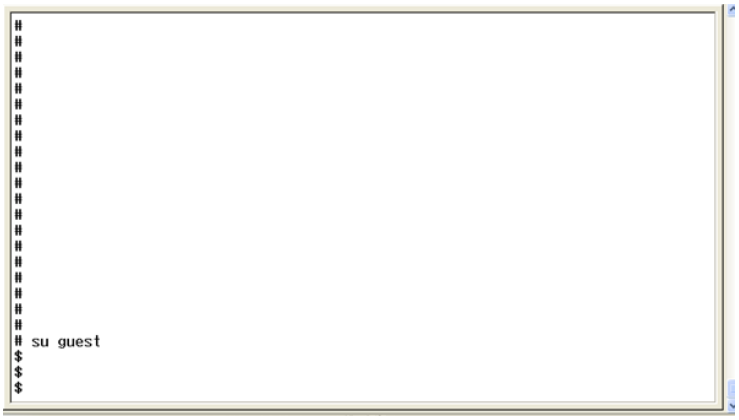


Figure 3.8 Switch to *guest*

3.3 Advidia Device Utility

Purpose:

To view and configure the device via LAN (Local Area Network), you need to connect the network device in the same subnet with your PC. Then install the Advidia Device Utility to find your Advidia Camera or Encoder

- The following figure shows the cable connection of a network camera and a PC:

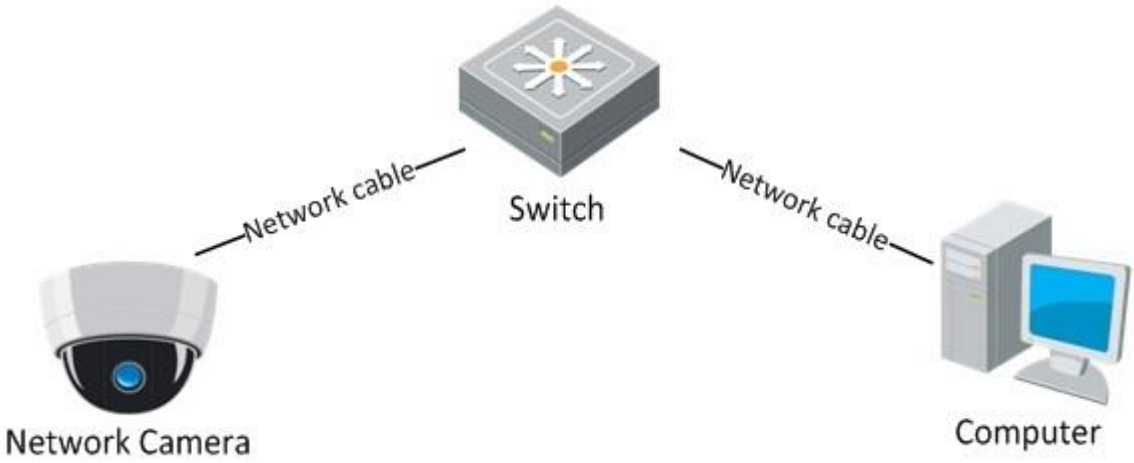


Figure 1-1 Wiring over LAN

- Set the IP address of the device for accessing via LAN.

Steps:

1. To get the IP address, you can choose either of the following method:
   - ♦ Use Advidia Device Utility, a software tool which can automatically detect Advidia devices in the LAN and list the device information like IP address, subnet mask, port number, device serial number, device version, etc., shown in Figure 1-2.
2. Change the IP address and subnet mask to the same subnet as of your PC.

Refer to the following introduction to set IP address with SADP software:

- ✧ **Search active devices online**

  Search online devices automatically:

  After launch the SADP software, it automatically searches the online devices every 15 seconds from the subnet where your computer locates. It displays the total number and information of the searched devices in the Online Devices interface. Device information including the device type, IP address, port number, gateway, etc. will be displayed.

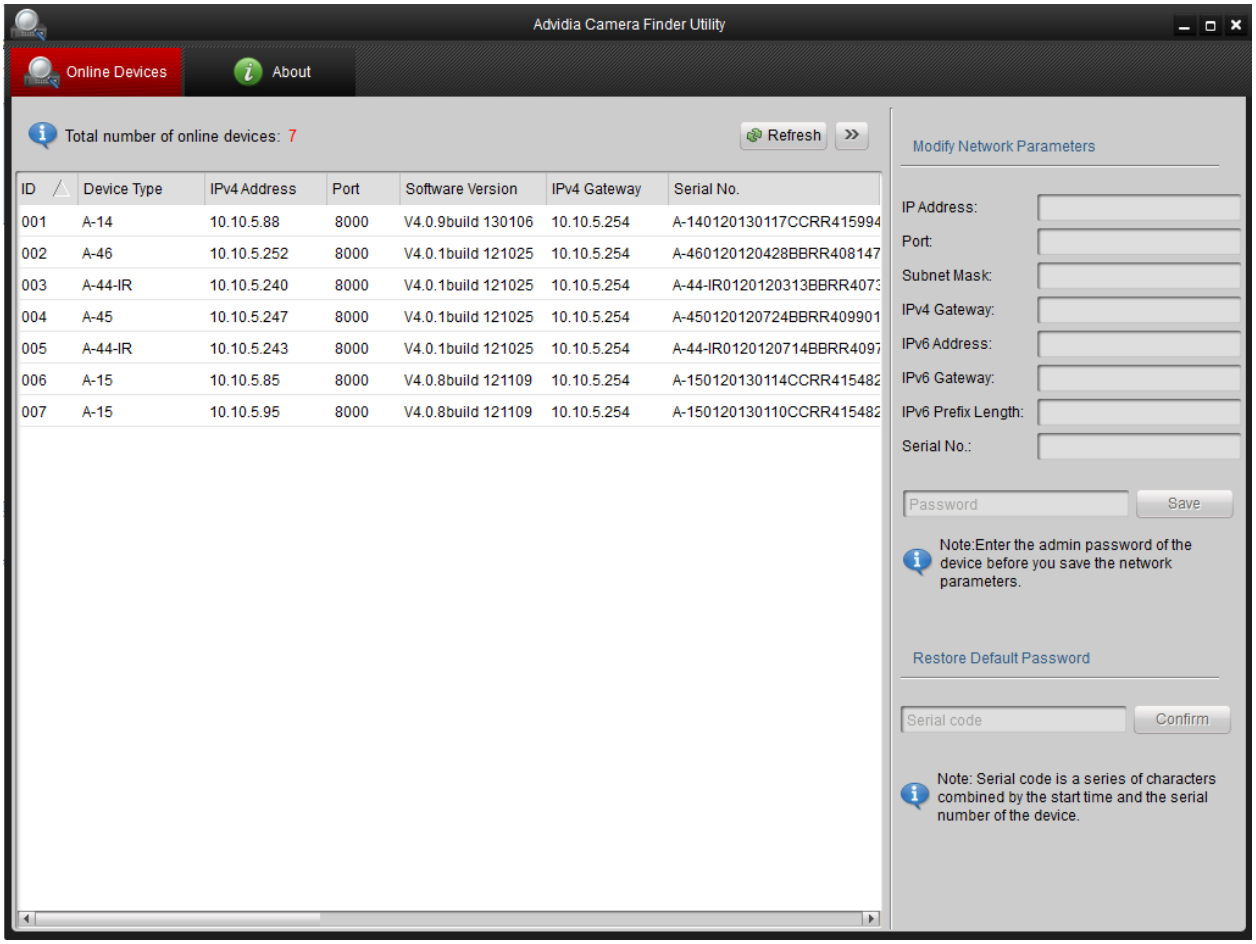

Advidia Camera Finder Utility
Online Devices
About
Total number of online devices: 7
Refresh
ID
Device Type
IPv4 Address
Port
Software Version
IPv4 Gateway
Serial No.
001 A-14 10.10.5.88 8000 V4.0.9build 130106 10.10.5.254 A-140120130117CCRR415994
002 A-46 10.10.5.252 8000 V4.0.1build 121025 10.10.5.254 A-460120120428BBRR408147
003 A-44-IR 10.10.5.240 8000 V4.0.1build 121025 10.10.5.254 A-44-IR0120120313BBRR4073
004 A-45 10.10.5.247 8000 V4.0.1build 121025 10.10.5.254 A-450120120724BBRR409901
005 A-44-IR 10.10.5.243 8000 V4.0.1build 121025 10.10.5.254 A-44-IR0120120714BBRR4097
006 A-15 10.10.5.85 8000 V4.0.8build 121109 10.10.5.254 A-150120130114CCRR415482
007 A-15 10.10.5.95 8000 V4.0.8build 121109 10.10.5.254 A-150120130110CCRR415482
Modify Network Parameters
IP Address:
Port:
Subnet Mask:
IPv4 Gateway:
IPv6 Address:
IPv6 Gateway:
IPv6 Prefix Length:
Serial No.:
Password
Save
Note:Enter the admin password of the device before you save the network parameters.
Restore Default Password
Serial code
Confirm
Note: Serial code is a series of characters combined by the start time and the serial number of the device.

Figure 1-2 Searching Online Devices

Note: Device can be searched and displayed in the list in 15 seconds after it goes online; it will be removed from the list in 45 seconds after it goes offline.

Search online devices manually:

You can also click Refresh to refresh the online device list manually. The newly searched devices will be added to the list.

Note: You can click △ or ▽ on each column heading to order the information; you can click » to show the device table and hide the network parameter panel on the right side, or click « to show the network parameter panel.

✧ **Modify device information**

Steps:

1) Select the device to be modified in the device list as shown in Figure 1-3. The network parameters of the device will be displayed

in the Modify Network Parameters panel on the right side as shown in Figure 1-4.

2) Edit the modifiable network parameters, e.g. IP address and port number.

3) Enter the password of the admin account of the device in the **Password** field and click Save to save the changes.

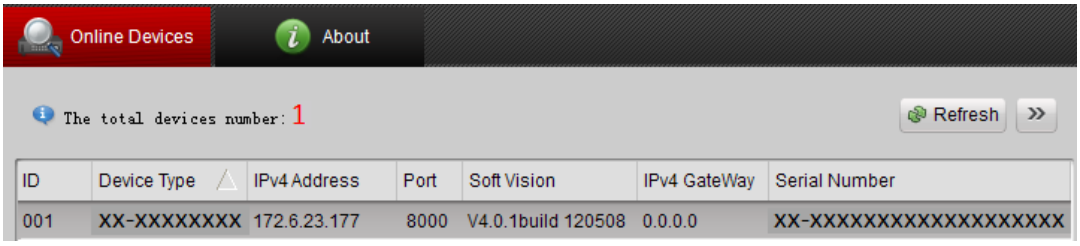


Figure 1-3 Select a Device

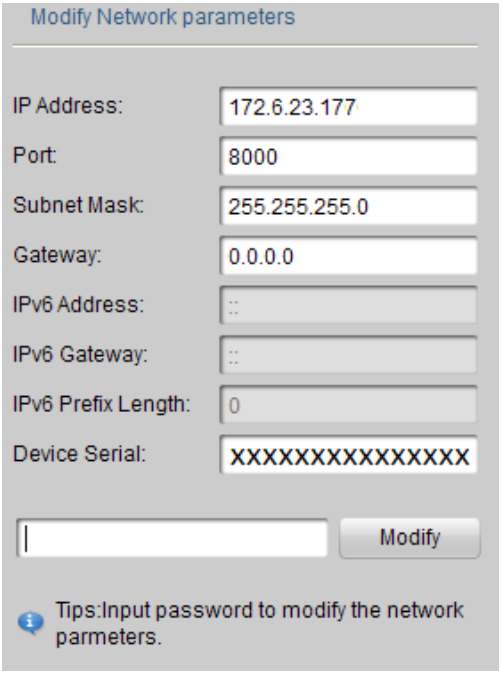


Figure 1-4 Modify Network Parameters

3. You can enter the IP address of network camera in the address field of the web browser to view the live video.

Note:

- The default value of the IP address is “192.0.0.64”. The default user name is “admin”, and password is “12345”.
- For accessing the network camera from different subnets, please set the gateway for the network camera after you log in.

Chapter 4 Access to VP-4 by WEB Browser

The VP-4 can also be accessed by WEB Browser for configuration and operation. The supported WEB browsers include: Internet Explorer 6/7/8/9, Firefox 3.5 and above, Chrome 8 and above, Safari 5.0.2 and above, Windows XP SP1 and above (32-bit).

Before you start:

- Before access, user needs to configure the network settings of device according to *Chapter 3*.
- Connect the device to the LAN, and prepare a PC connected to the same LAN with the device.
- The factory default username of the device is *admin* and the password is *12345*.
- The factory default IP address of the device is *192.0.0.64*.

5.1 Installing Web Components

Steps:

1. Open WEB browser, input the IP address of VP-4 (e.g., http://192.0.0.64) and then press the **Enter** key on PC. The system then will display the login interface:

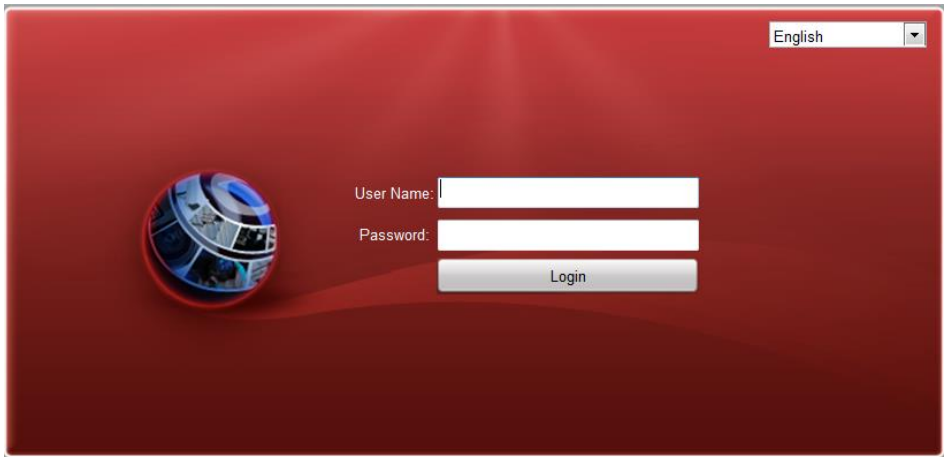


Figure 5.1 Login Page

Input the user name (default: admin) and password (default: 12345) to log into the system.

2. On the main page of VP-4, you need to download and install the plug-in.
   (1) Click on the live view panel by following the hints on the screen.

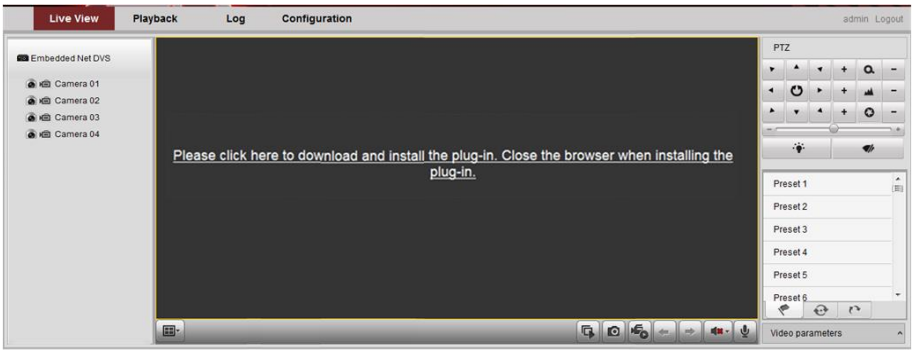


Figure 5.2 Download and Install Plug-in

(2) Click **Run** or **Save** on the pop-up warning message box.

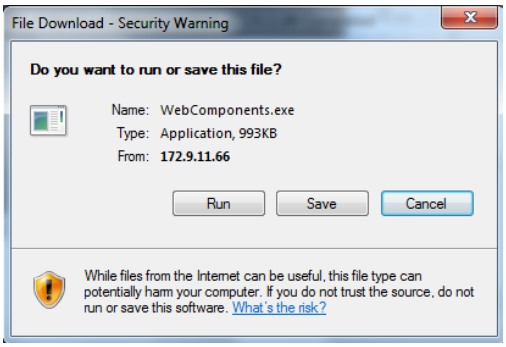

File Download - Security Warning
Do you want to run or save this file?
Name: WebComponents.exe
Type: Application, 993KB
From: 172.9.11.66
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Figure 5.3 Run WebComponents

(3) Click **Next** on the pop-up Setup dialog box.

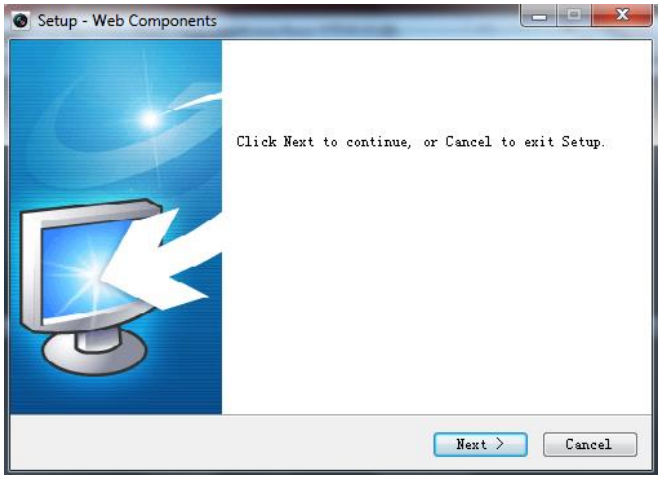


Figure 5.4 Click Next

(4) When the installation completes, click **Finish** to finish the installation of Web Components.

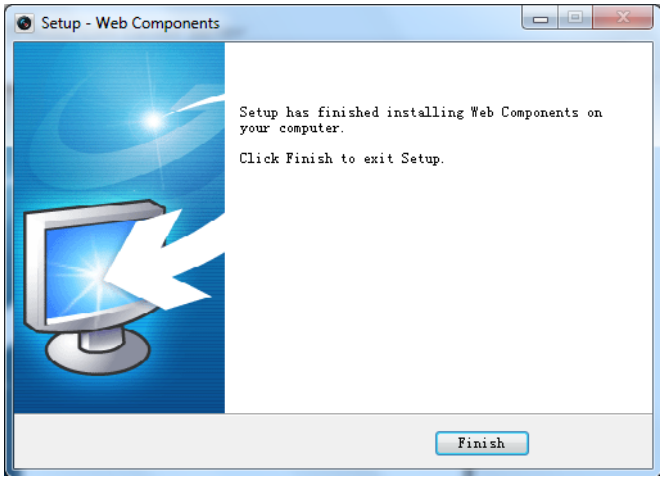


Figure 5.5 Finish the Setup

5.2 Main Page

After successful login, you will enter the main page automatically.

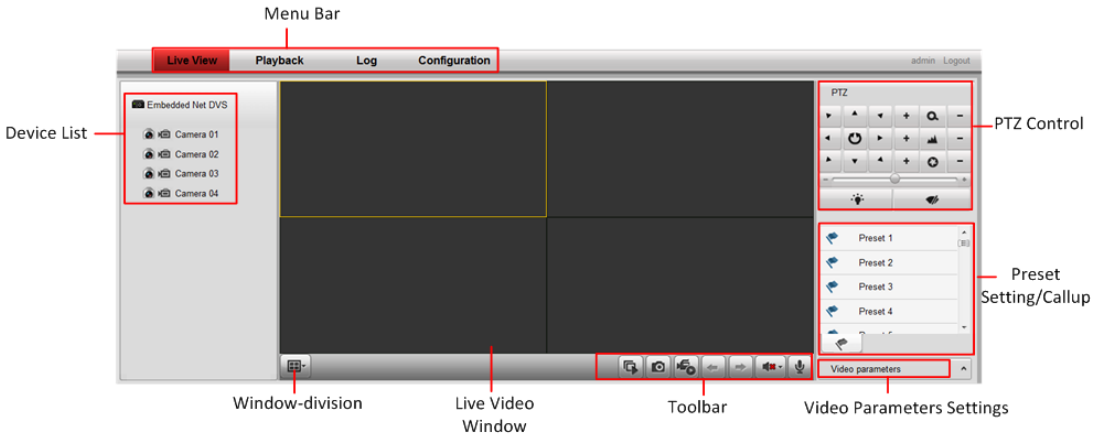


Figure 5.6 Main Page

Description of the live view page:

Menu Bar: Enter the Live View, Playback, Log and Configuration page respectively.

Device List: Display the connected encoder and its channels.

Window-division: 1/4-division display mode.

Live Video Window: Display the live video of the current camera.

Toolbar: Realize functions in live view mode, e.g., live view, capture, recording, audio on/off, two-way audio, etc.

PTZ Control: Realize PTZ control of the camera (supports PTZ function), and the lighter and wiper control.

Preset Setting/Callup: Set and call the preset for the camera (supports PTZ function).

Video Parameters Settings: Configure the brightness, contrast, hue and saturation of the live video.

Chapter 5 Live View

Live view shows you the video image getting from the connected camera in real time. After successful login, the system will enter the live view page automatically.

5.1 Starting Live View

Steps:

1. In the live view window, select a playing window by clicking the mouse.
2. Double click a camera from the device list to start the live view.

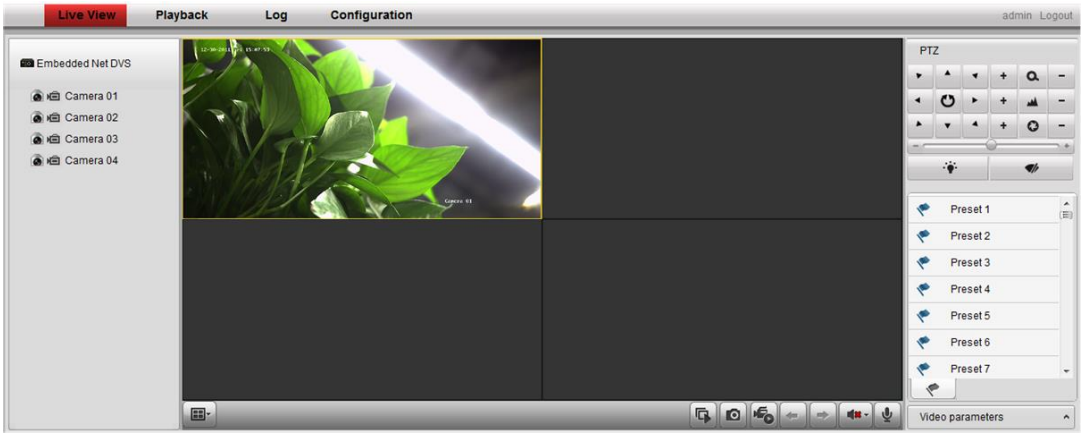


Figure 5.1 Start Live View

3. You can click the button on the toolbar to start the live view of all cameras on the device list.

Refer to the following table for the description of buttons on the live view window:

Table 5.1 Description of Toolbar

Icon	Description
	Select the window-division mode to 1×1 or 2×2.
/	Star/Stop live view
	Capture pictures in live view mode
/	Manually start/stop recording
	Previous page
	Next page
/	Audio on/off
/	Start/Stop two-way audio

Note: Before using two-way audio function or recording with audio, please select the **Stream Type** to **Video & Audio** on *Section 7.2 Configuring Video Settings.*

Full-screen Mode

You can double click on the live video to switch to the full-screen view mode. To switch back to the normal mode, double click on the live video again.

Please refer to the following section for more information:

1. Capturing pictures on *Section*
2. *5.2 Capturing* Picture. .
3. Configuring recording on ***Error! Reference source not found.***.
4. Setting the image quality of live view on *Section 6.1 Local Configuration*.
5. Setting the saving path for the recorded video files and captured pictures on *Section 6.1 Local Configuration..*
6. Setting the OSD text on live video on *Section 7.1 Configuring OSD Settings*. .

5.2 Capturing Picture

In live view mode, click the button on the toolbar to capture the live pictures.

When the picture is captured, the following pop-up message box will appear at the lower right corner.

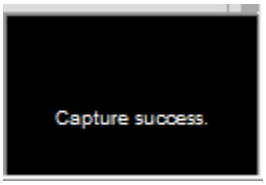


Figure 5.2 Capture Picture

***Note*:**

1. The saving path for the captured pictures can be set at the **Configuration > Local Configuration** page.
2. The image is saved as a JPEG file on your computer.

5.4 Operating PTZ Control

Before you start:

1. Make sure the encoder is connected with the camera/dome which supports PTZ function. Connect the *R*+ and *R*- terminals of the pan/tilt unit or speed dome to RS-485 T+ and RS-485 T- terminals of the VP-4 respectively.
2. The baud rate, PTZ control and address configured in the **RS-485 Settings** interface (**Remote Configuration > Serial Port Settings > 485 Serial Port**), as shown in Figure 6.3, must be the same with the parameters of the connected pan/tilt unit or speed dome.

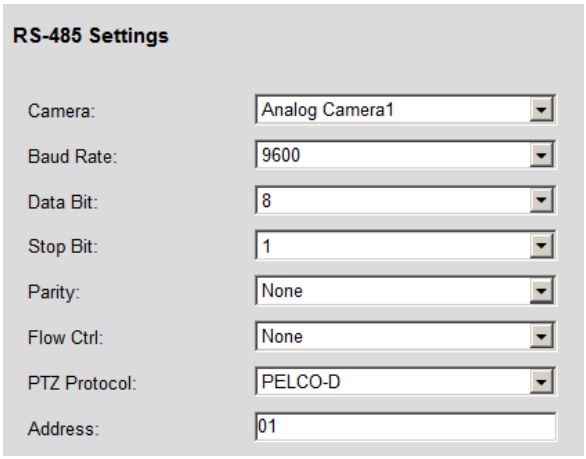


Figure 5.3 RS-485 Settings

5.4.1 Operating PTZ Control

In live view mode, you are allowed to use the PTZ control buttons to realize pan/tilt/zoom control of the camera lens.

There are 8 directional buttons (up, down, left, right, upper left, upper right, bottom left, bottom right) on the display window when the mouse is located in the relative positions.

Click on the directional buttons to control the pan/tilt movement.

Figure 5.4 PTZ Control Panel

Click the zoom/iris/focus buttons to realize lens control.

Refer to the following table for description of PTZ control buttons:

Table 5.1 Description of PTZ Control Buttons

Button	Description
	Zoom in/out
	Focus near/far
	Iris open/close
	Light
	Wiper
	Adjust speed of pan/tilt movement

5.4.2 Setting / Calling A Preset

Setting a Preset:

1. In live view mode, select a preset number from the preset list.

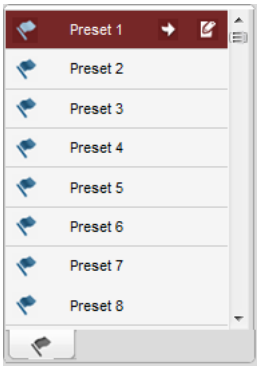


Figure 5.5 Set a Preset

2. Use the PTZ control buttons to move the lens in the desired position. You can use any of the following commands:
   - Pan the camera to the right or left.
   - Tilt the camera up or down.
   - Zoom in or out.
   - Refocus the lens.
3. Click the icon to finish the setting of current preset.

***Note*:** Up to 256 presets can be configured.

Calling a Preset:

This feature enables the camera to point to a specified preset scene when an event takes place. For the pre-defined preset, you can call it at any time to the desired preset scene.

In live view mode, select a predefined preset from the list and click the icon to call a preset.

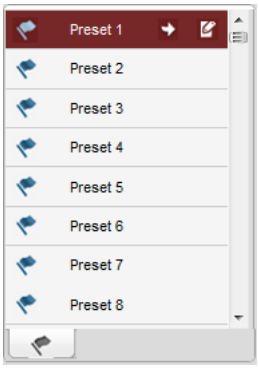


Figure 5.6 Call a Preset

Linking to Alarm:

The preset can also be used to link to the alarm input when there is alarm event occurring.

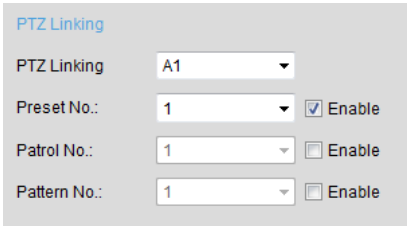


Figure 5.7 PTZ Linking

Please refer to *Chapter 7.3 Configuring and Handling Alarms* for the PTZ Linking settings (Remote Configuration>Alarm Settings>Alarm Input>Linking Method).

5.5 Configuring Video Parameters

Purpose:

You can configure the OSD (On-screen Display) settings for the camera, including date /time, camera name, etc.

Steps:

1. In the live view interface, click the Video parameters button on the bottom right corner to spread the Video Parameters Setting interface:

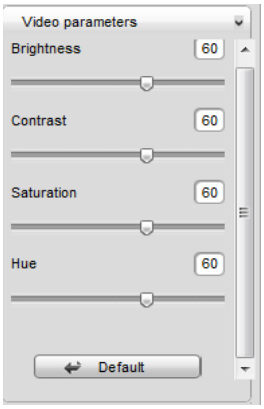


Figure 5.8 Video Parameters Settings

2. Move the slider to adjust the brightness, contrast, saturation and hue.

   ***Note*:** The range of adjustment is 0 to 100; the default setting is 60.

   You can also click the Default button to restore the default settings.

Chapter 6 Device Configuration

6.1 Local Configuration

Click **Configuration > Local Configuration** to enter the Local Configuration interface.

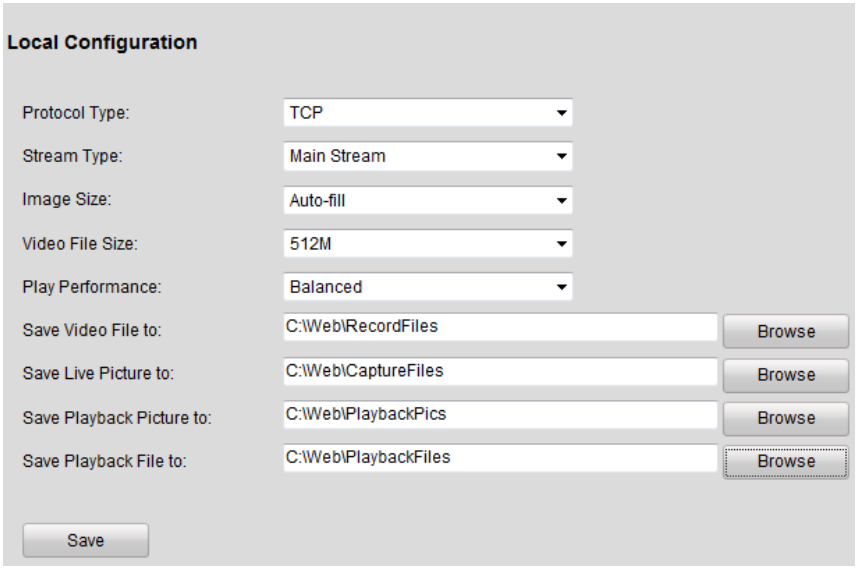


Figure 6.1 Local Configuration

Configure the following settings:

Protocol Type: Set the protocol type of stream transmission to TCP or UDP.

- **UDP:** provides more real-time audio and video streams.
- **TCP:** ensures complete deliver of streaming data and better video quality, yet its real-time effect is not so good.

Stream Type: Select the stream type to main stream or sub stream used for live view by Web browser. Please refer to *Section 7.2 Configuring Video Settings* for the parameters settings of the main stream and sub stream respectively.

Image Size: Select the window-division view mode to 4:3, 16:9 or Auto-fill.

Video File Size: Select the size of packed video files during manual recording to 256M, 512M or 1G.

Play Performance: Set the live viewing performance to Least Delay, Balanced (delay and fluency) or Best Fluency.

Save Video File to: Set the saving path for the manually recorded video files.

Save Live Pictures to: Set the saving path for the manually captured pictures in live view mode.

Save Playback Picture to: Set the saving path for the captured pictures in playback mode.

Save Playback File to: Set the saving path for the clipped video files in playback mode.

***Note*:** You can click the **Browse** button to change the directory for saving the video files and pictures.

6.2 Configuring Time Settings

Steps:

1. Click **Remote Configuration > Device Parameters > Time Settings** to enter the Time Settings interface:

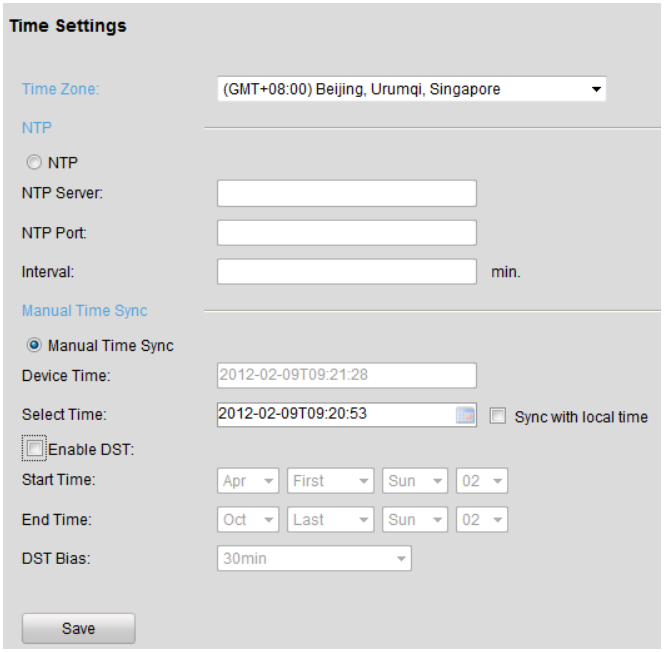


Figure 6.2 Time Settings

2. Select the Time Zone.

Select the Time Zone that is closest to the device's location from the drop-down menu.

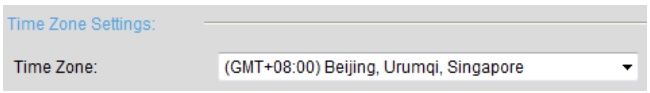


Figure 6.3 Time Zone Settings

3. Configure the time synchronization by NTP server or by manually.

- **Configuring Time Sync by NTP Server**

A Network Time Protocol (NTP) Server can be configured on your device to ensure the accuracy of system date/time.

If the device is connected to a Dynamic Host Configuration Protocol (DHCP) network that has time server properties configured, the camera will synchronize automatically with the time server.

Enable the **NTP** function by checking the checkbox, and configure the following settings:

NTP Server: IP address of NTP server.

NTP Port: Port of NTP server.

Interval: The time interval between the two synchronizing actions with NTP server. It can be set from 1 to 10080 minutes.

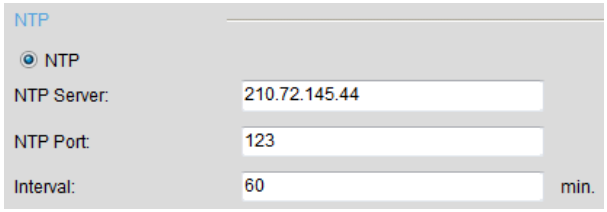


Figure 6.4 Time Sync by NTP Server

***Note*:** If the device is connected to a public network, you should use a NTP server that has a time

synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the device is set up in a more customized network, NTP software can be used to establish a NTP server used for time synchronization.

- Configuring Time Synchronization by Manually

Enable the **Manual Time Sync** function and then click the icon to set the system time from the pop-up calendar. You can check the checkbox of **Snyc with local time** to synchronize the time with the local PC.

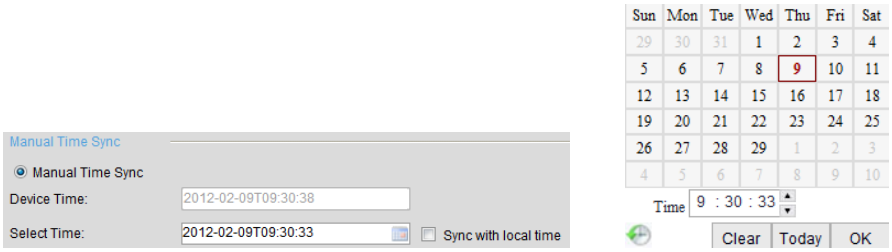

Manual Time Sync
Manual Time Sync
Device Time:
2012-02-09T09:30:38
Select Time:
2012-02-09T09:30:33
Sync with local time
Sun Mon Tue Wed Thu Fri Sat
29 30 31 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 1 2 3
4 5 6 7 8 9 10
Time 9 : 30 : 33
Clear Today OK

Figure 6.5 Time Sync by Manually

4. Configure DST settings if needed.

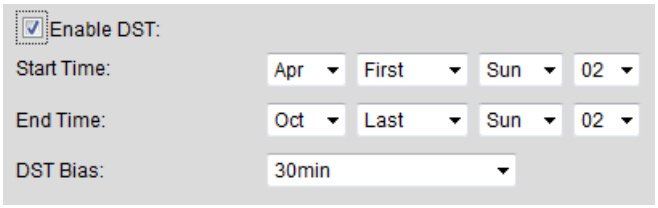


Figure 6.6 Set DST

(1) Check the checkbox before the **Enable DST**.

(2) Set the start tine and end time of DST period. The end time must be later than the start time. When the DST period ends, the system will reverts to the standard local time.

(3) Set the DST bias to 30min, 60min, 90min or 120min.

5. Click the **Save** button to save the settings.

6.3 Network Settings

6.3.1 Configuring Basic Settings

Network settings must be properly configured before you operate device over network.

Steps:

1. Click the **Remote Configuration > Network Settings > Basic Settings** to enter the Basic Network Settings interface:

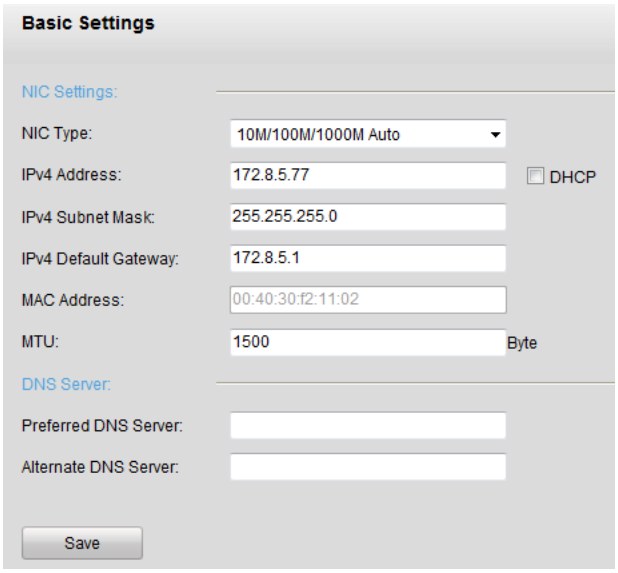


Figure 6.7 Basic Network Settings

2. Configure the NIC settings, including the NIC Type, IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway, and MTU settings.

Note: The valid value range of MTU is 500 ~ 9676.

3. If the DHCP server is available, you can click the checkbox of DHCP to automatically obtain an IP address and other network settings from that server.
4. If the DNS server settings are required for some applications (e.g., sending email), you should properly configure the Preferred DNS Server and Alternate DNS Sever here.

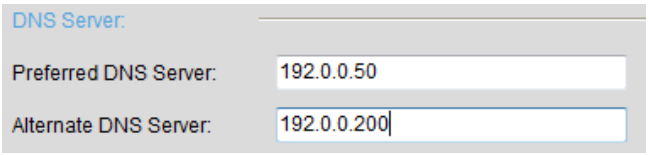


Figure 6.8 DNS Server Settings

5. Click the **Save** button to save the above settings.

6.3.2 Configuring PPPoE Settings

Your device also allows access by Point-to-Point Protocol over Ethernet (PPPoE).

Steps:

1. Click the **Remote Configuration > Network Settings > PPPoE Settings** to enter the PPPoE Settings interface:

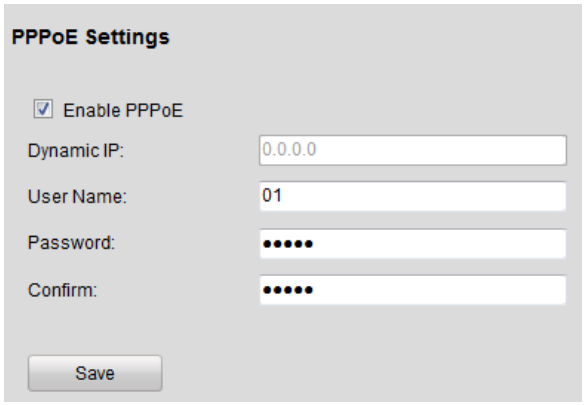


Figure 6.9 PPPoE Settings

2. Check the **PPPoE** checkbox to enable this feature.
3. Enter **User Name**, **Password**, and **Confirm Password** for PPPoE access.

Note: The User Name and Password should be assigned by your ISP.

4. Click the **Save** button to save and exit the interface.

6.3.3 Configuring DDNS Settings

If your device is set to use PPPoE as its default network connection, you may set Dynamic DNS (DDNS) to be used for network access.

Prior registration with your DDNS Provider is required before configuring the system to use DDNS.

Steps:

1. Click the **Remote Configuration > Network Settings > DDNS Settings** to enter the DDNS Settings interface:

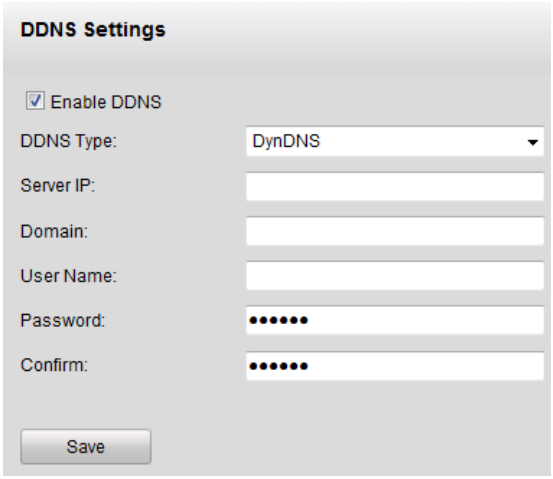


Figure 6.10 DDNS Settings

2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Four different DDNS types are selectable: IPServer, DynDNS, PeanutHull and NO-IP.
   - **DynDNS:**

   (1) Enter **Server Address** for DynDNS (e.g. members.dyndns.org).

   (2) In the **Device Domain Name** text field, enter the domain obtained from the DynDNS website.

(3) Enter the **User Name** and **Password** registered in the DynDNS website.
(4) Click **Save** to save the settings.

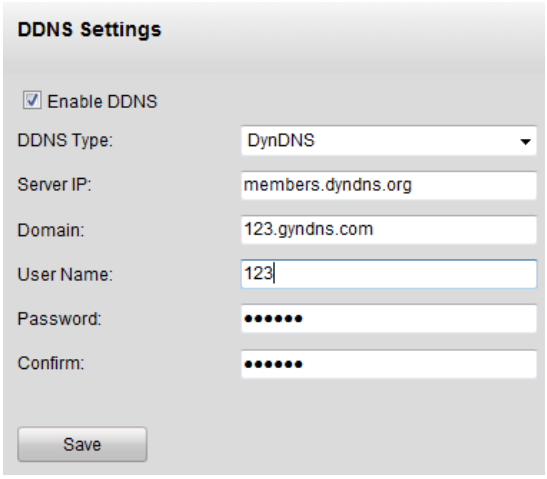


Figure 6.11 DynDNS Settings

- **IPServer:**

(1) Enter Server Address for IPServer.
(2) Click **Save** to save the settings.
Note: For the IP Server, You have to apply a static IP, subnet mask, gateway and primary DNS from the ISP. The **Server IP** should be entered with the static IP address of the PC that runs IPServer software.

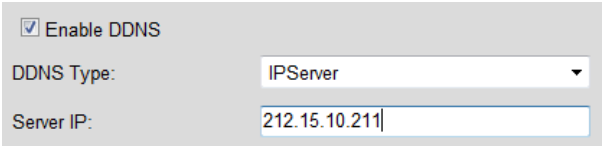


Figure 6.12 IPServer Settings

- **PeanutHull:**

(1) Enter User Name and Password obtained from the PeanutHull website.
(2) Click **Save** to save the settings.

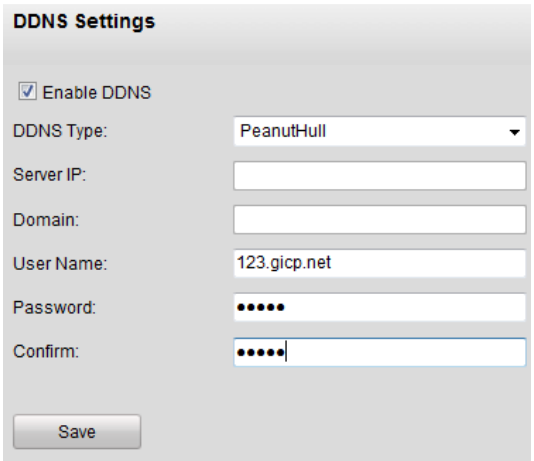


Figure 6.13 PeanutHull Settings

- **NO-IP:**

  (1) Enter the Server Address for NO-IP.

  (2) In the **Domain Name** text field, enter the domain obtained from the NO-IP website (www.no-ip.com).

  (3) Enter the **User Name** and **Password** registered on the NO-IP website.

  (4) Click **Save** to save the settings.

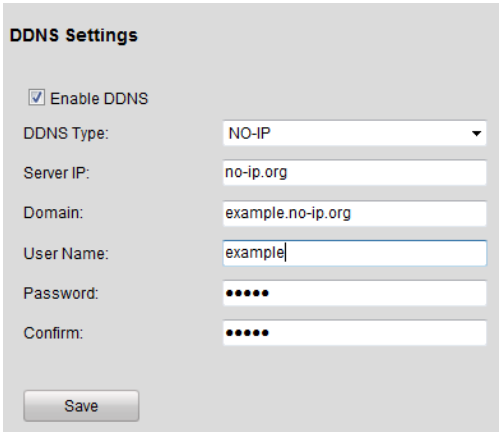


Figure 7.14 NO-IP Settings

6.3.4 Configuring Email Settings

Purpose:

The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, tamper-proof, etc.

Before you start

1. Before configuring the Email settings, the device must be connected to a local area network (LAN) that maintains an SMTP mail server. The network must also be connected to either an intranet or the Internet depending on the location of the e-mail accounts to which you want to send notification.
2. Please configure the DNS Server settings under **Remote Settings>Network Settings>Basic Settings** before using the Email function.

Steps:

1. Enter the Basic Network Settings (**Remote Configuration > Network Settings > Basic Settings)** to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.
2. Click the **Remote Configuration > Network Settings > Email Settings** to enter the Email Settings interface:

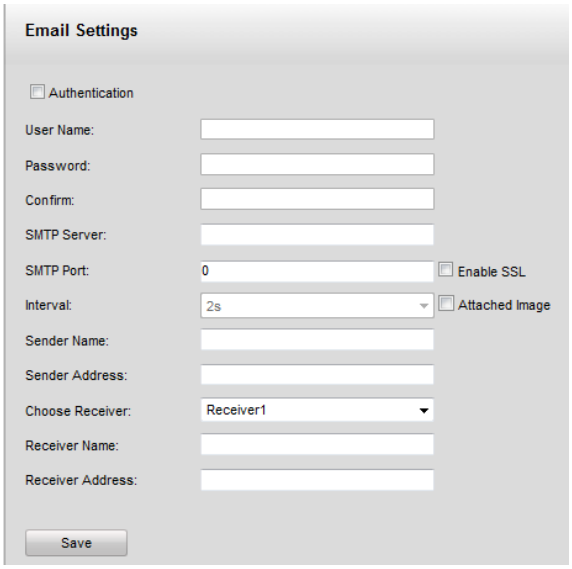


Figure 6.15 Email Settings (1)

3. Configure the following Email settings:

Authentication (optional): If your mail server requires authentication, check this checkbox to use authentication to log in to this server and enter the login User Name and Password.

SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

SMTP Port: The SMTP port. The default TCP/IP port used for SMTP is 25.

Enable SSL: Click the checkbox to enable SSL if required by the SMTP server.

Interval: The interval refers to the time between two actions of sending attached pictures.

Attached Image: Check the checkbox of **Attached Image** if you want to send email with attached alarm images.

Sender Name: The name of sender.

Sender Address: The Email address of sender.

Choose Receiver: Select the receiver to which the Email is sent. Up to 3 receivers can be configured.

Receiver Name: The name of user to be notified.

Receiver Address: The Email address of user to be notified.

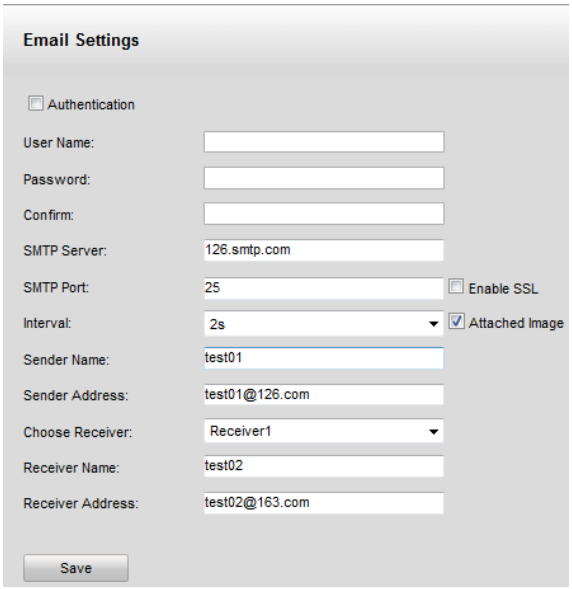


Figure 6.16 Email Settings (2)

4. Click **Save** to save the Email settings.

Please refer to the following sections for more information:

- Configuring alarm linking method with **Send Email** on *Section 7.3.1 Configuring Motion Detection*.
- Configuring alarm linking method with **Send Email** on *Section 7.3.2 Configuring External Alarm Input.*
- Configuring alarm linking method with **Send Email** on *Section 7.3.3 Configuring Video Loss Alarm.*
- Configuring alarm linking method with **Send Email** on *Section 7.3.4 Configuring Tamper-proof Alarm.*
- Configuring alarm linking method with **Send Email** on *Section 7.3.5 Handling Exception.*

6.3.5 Adding Network Disk

For VP-4HCI/HFI models, you should configure the network disk before operating the recording, playback or log searching. For other models with SATA disks connected, the configuration of network disk is selectable.

Before you start:

1. The network storage device is available within the network and is properly connected.
2. The network storage device is configured with NAS or IP SAN mode (please refer to the User Manual of IP SAN/NAS).

Steps:

1. Click **Remote Configuration > Network Settings >NetHDD Settings** to enter the NetHDD Settings interface.

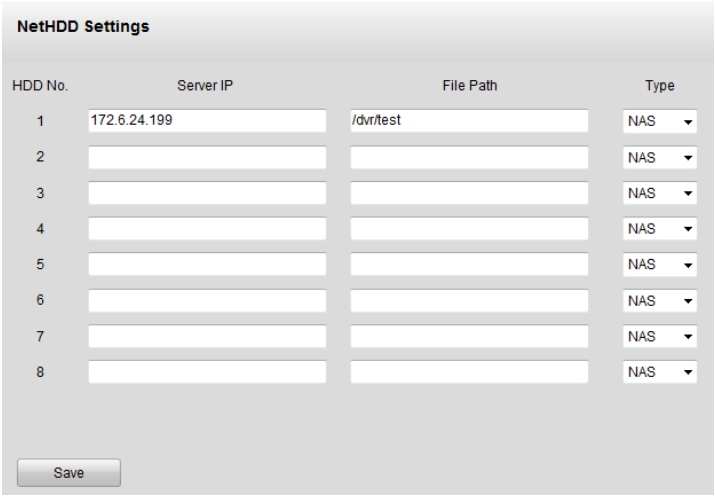


Figure 6.17 Network Disk Settings

2. Enter the IP address of the Network Storage System and File Path in the text filed.
3. Select the type of Network Storage System to IP SAN or NAS.

   NAS Mode: Enter the IP address of the storage device, and the default file path is */dvr/share*, in which the *share* name is user-defined during creating the DVR of the network storage.

   IP SAN mode: Enter the IP address of the storage device, and the default file path is *iqn.2004-05.storos.t-service ID*, in which the *service ID* is user-defined during creating the iSCSI volume of the network storage.
4. Click the **Save** button to add the configured network disk.
5. Initialize the added network disk.

(1) Click **Remote Configuration > HDD Management** to enter the HDD settings menu, on which you

can view the capacity, free space, status, type and property of the added network disk.

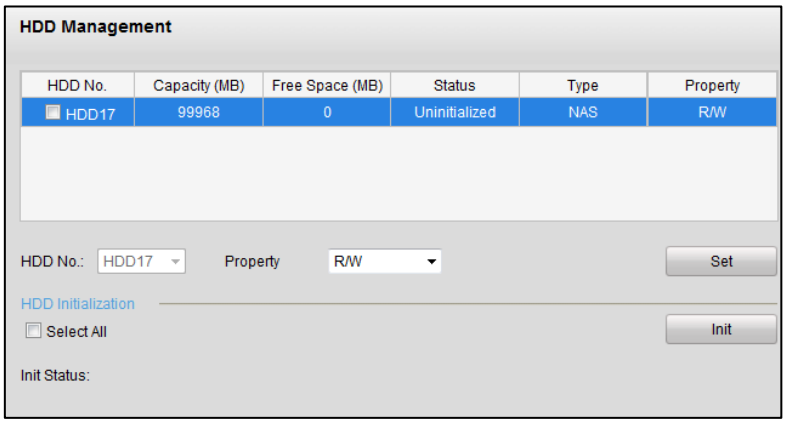


Figure 6.18 Initial Disk

(2) If the status of the network disk is **Uninitialized**, select the disk from the list by checking the checkbox and click the **Init** button to start initializing the disk.

(3) When the initialization is complete, the status of disk will become **Normal.**

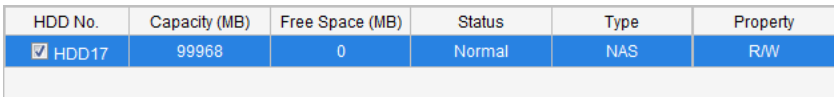


Figure 6.19 HDD Status-Normal

6. Set the property of the added network disk.

Select the HDD No., and select the property from the drop-down menu to R/W, Read-only or Redundancy.

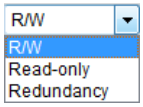


Figure 6.20 Set HDD Property

***Note*:**

1. Please refer to the User Manual of IP SAN/NAS for the creation of File Path in the network management.
2. Up to 8 NAS disks or IP SAN disk can be connected to the VP-4.

6.3.6 Configuring SNMP Settings

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks.

Steps:

1. Click **Remote Configuration > Network Settings >SNMP Settings** to enter the SNMP Settings interface.
2. Select the NIC port (default: 161).
3. When the SNMPv1 or SNMP v2c is enabled (or both enabled), you can configure the read SNMP community (default: public), write SNMP community (default: private), tap address (default: empty)

and trap port (default: 162).

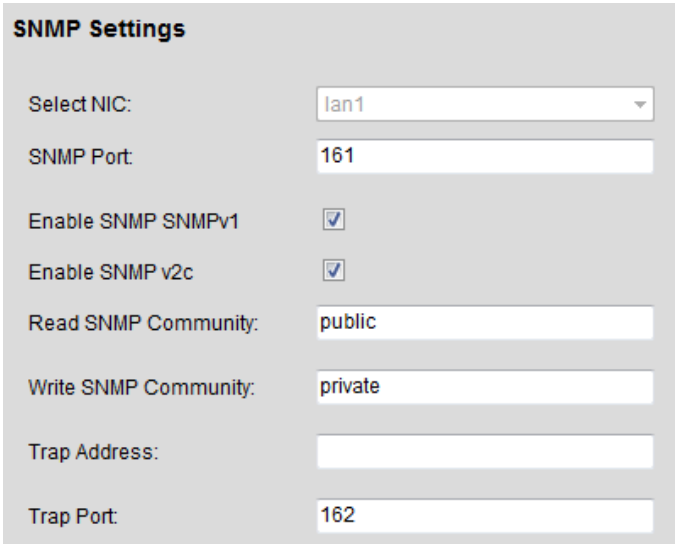


Figure 6.21 SNMP Settings (1)

4. When the SNMPv3 is enabled, you can configure the read username (default: public).

   ***Note*:** By default settings, the SNMPv1, SNMP v2c and SNMPv3 are disabled.

5. Select the security level to “no auth, no priv”, “auth, no priv”, “no auth, priv” or “auth, priv”.

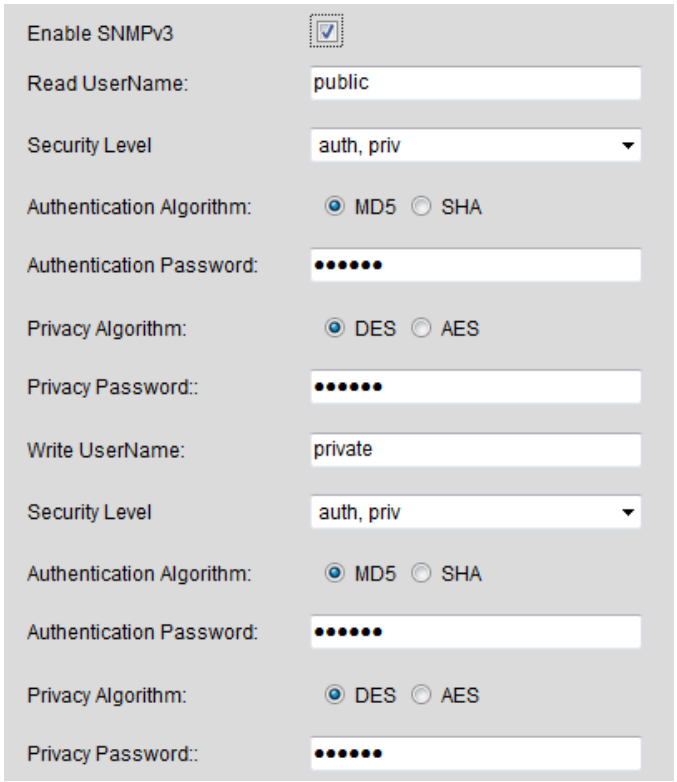


Figure 6.22 SNMP Settings (2)

6. (1) When the security level is set to “**auth, priv”**, you can configure the Authentication Algorithm and Privacy Algorithm parameters.

(2) When the security level is set to “**no auth, no priv**”, you cannot configure the Authentication Algorithm and Privacy Algorithm parameters.

7. Click **Save** to save the above settings.

Chapter 7 Camera Settings

7.1 Configuring OSD Settings

7.1.1 Configuring Display Settings

Purpose:

You can customize the camera name and time on the screen.

Steps:

1. Click the **Remote Configuration >Camera Settings > Display Settings** to enter the Display Settings interface:

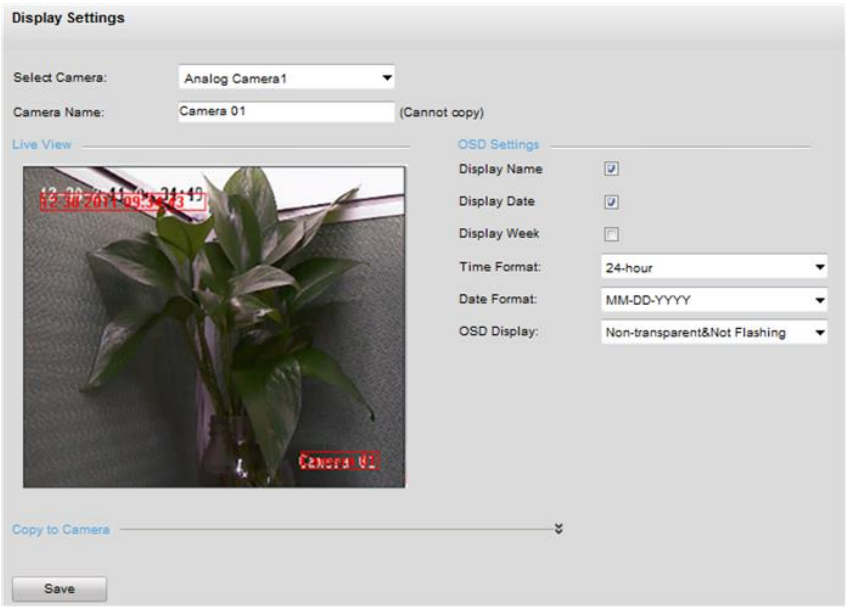


Figure 7.1 Display Settings

2. Select the camera from the drop-down list.
3. Edit the camera name in the text field of Camera Name.

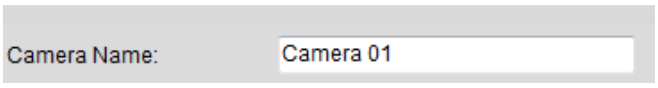


Figure 7.2 Edit Camera Name

4. Select the display of camera name, date or week by checking the checkboxes if required.
5. Set the time format, date format and OSD display mode by selecting option from the drop-down list.
6. Configure the OSD size to large, middle or small.
7. On the preview image, you can adjust the OSD location on the screen by moving the text frame.

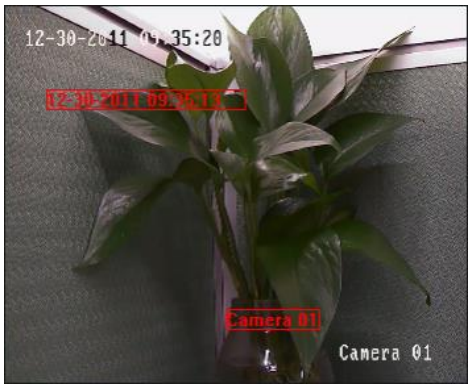


Figure 7.3 Adjust OSD Location

8. If you want to copy the display settings of the current camera to other cameras, spread the **Copy to Camera** panel and select the camera(s) to copy, or click **Select All** to select all cameras.

Figure 7.4 Copy to Camera

9. Click **Save** to validate the above settings.

7.1.2 Configuring Text Overlay

Steps:

1. Click the **Remote Configuration >Camera Settings > Text Overlay Settings** to enter the Text Overlay Settings interface.
2. Select the camera from the drop-down list.
3. Edit the user-defined text content.
   Click the checkbox in the text box below and then input the characters.
4. On the preview image, you can adjust the Text location on the screen by moving the text frame.

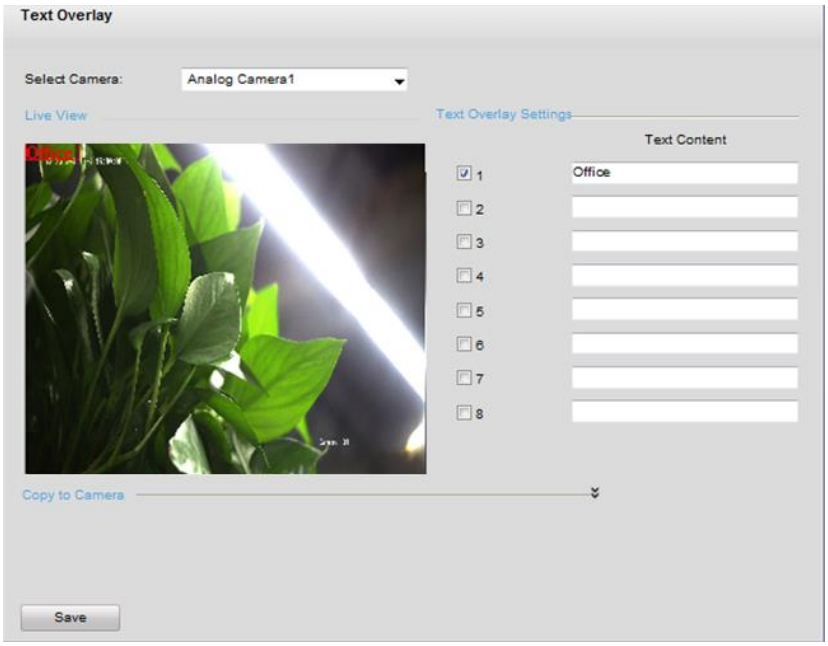


Figure 7.5 Text Overlay Settings

5. If you want to copy the text overlay settings of the current camera to other cameras, spread the **Copy to Camera** panel and select the camera(s) to copy, or click **Select All** to select all cameras.

Figure 7.6 Text Overlay Settings

6. Click **Save** to validate the above settings.

7.2 Configuring Video Settings

Steps:

1. Click **Remote Configuration > Camera Settings >Video Settings** to enter the Video Settings interface:

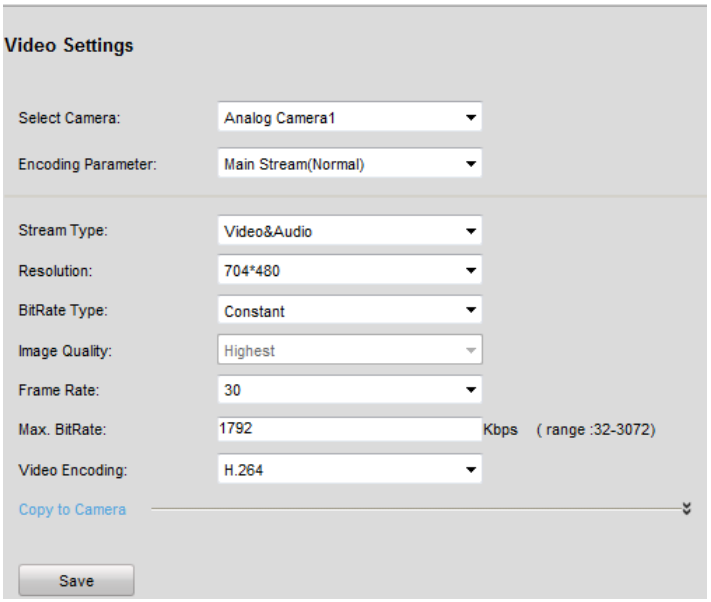


Figure 7.7 Video Settings

2. Select the camera from the drop-down list to configure.
3. Select the **Encoding Parameter** of the camera to Main Stream (Normal), Main Stream (Event) or Sub Stream.

   The main stream is usually for recording and live viewing with good bandwidth, and the sub stream can be used for live viewing when the bandwidth is low. Refer to the *Chapter 6.1 Local Configuration* on changing the main stream to sub stream for live viewing.
4. You can customize the following parameters for the selected Main Stream or Sub Stream:

   Stream Type: Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Stream Type** is **Video & Audio**.

   Resolution: Select the resolution of the video input.

   BitRate Type: Select the bitrate type to constant or variable.

   Image Quality: When bitrate type is selected to **Constant**, 6 levels of image quality can be configured.

   Frame Rate: Set the frame rate to 1~25 fps.

   The frame rate used to describe the frequency at which a video stream is updated is measured in frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

   Max. BitRate: Set the Max. bitrate to 32~3072 Kbps.

   Video Encoding: Select the video encoding standard to H.264.
5. If you want to copy the display settings of the current camera to other cameras, spread the **Copy to Camera** panel and select the camera(s) to copy, or click **Select All** to select all cameras.

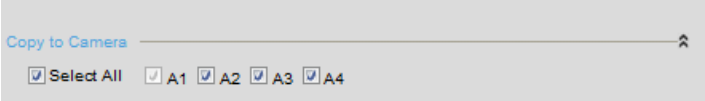


Figure 7.8 Copy to Camera

7. Click **Save** to save the above settings.

7.3 Configuring and Handling Alarms

Purpose:

This section explains how to configure the network camera to respond to alarm events, including Motion Detection, External Alarm Input, Video Loss, Tamper-proof and Exception. And the alarm events can trigger the alarm actions, such as Notify Surveillance Center, Send Email and Trigger Alarm Output.

7.3.1 Configuring Motion Detection

Motion detection is a feature which can alert the personnel and record the video for the motion occurred in the surveillance scene.

Steps:

1. **Set the Motion Detection Area**

   Steps:

   (1) Click **Remote Configuration> Camera Settings> Motion Detection** to enter the motion detection settings interface.

   (2) Select the camera to configure the motion detection.

   (3) Check the checkbox of **Enable Motion Detection**.

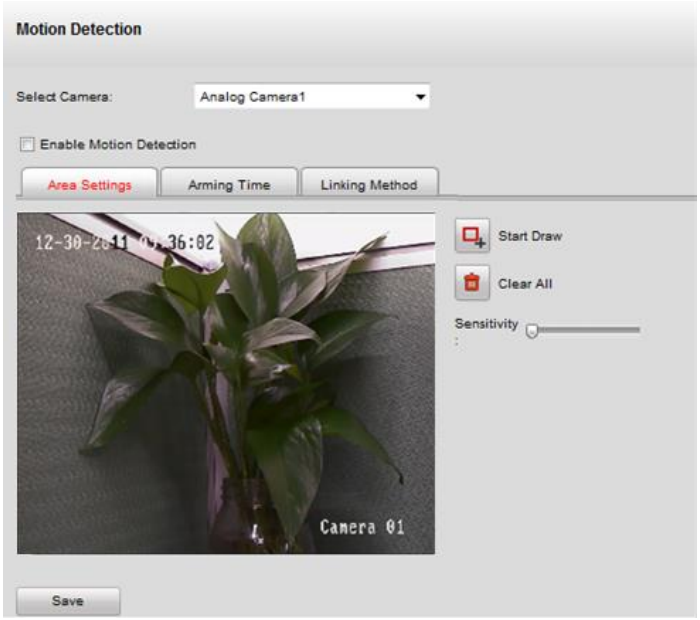


Figure 7.9 Motion Detection Settings

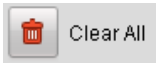
(4) Click the

button. Draw motion detection area by clicking and dragging the mouse in the live video image.

Note: You are allowed to draw 8 motion detection areas in the same image.

(5) Click the

button to finish drawing.

You can click the 

button to clear all areas.

(6) Move the slide bar

to set the sensitivity of the camera.

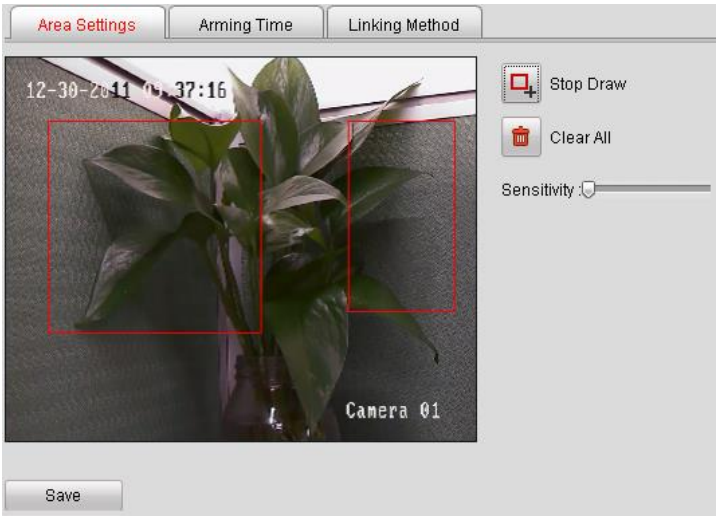


Figure 7.10 Motion Detection-Area Settings

(7) Click **Save** button to save the settings.

2. **Set the Arming Schedule for Motion Detection**

Steps:

(1) Click the **Arming Time** tab.

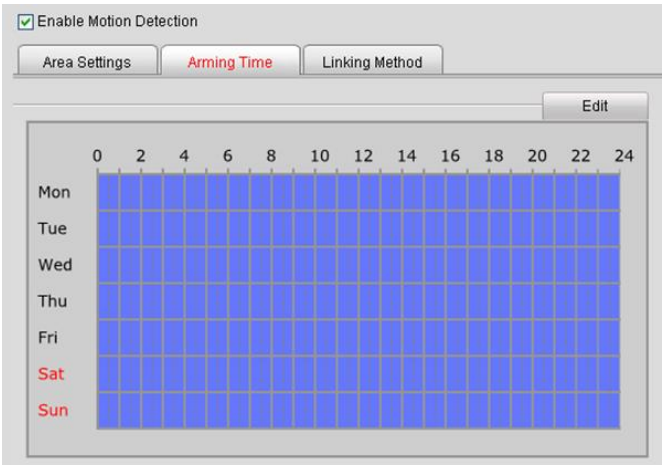


Figure 7.11 Motion Detection-Arming Time Settings

(2) Click the **Edit** button to edit the arming schedule.

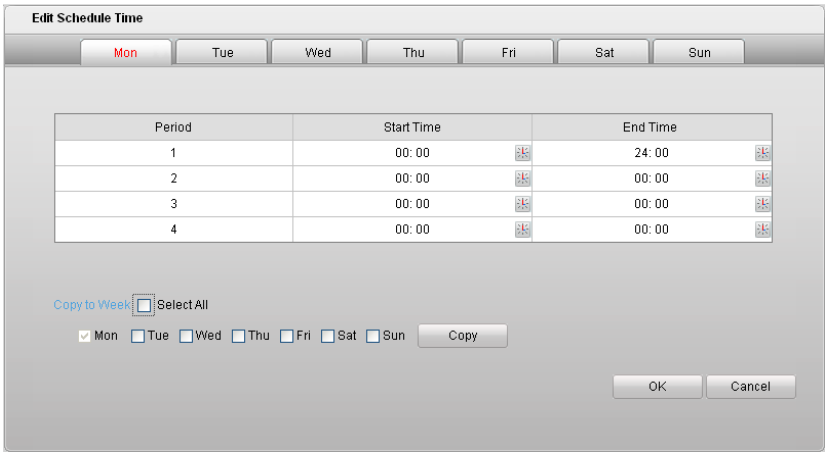


Figure 7.12 Motion Detection-Edit Arming Schedule

(3) Choose the day you want to set the arming schedule.

(4) Click the button to set the time period for the arming schedule.

(5) After you set the arming schedule, you can copy the schedule to other days.(Optional)

(6) Click **OK** button to save the settings.

Note: The time of each segment can't be overlapped. Up to 8 segments can be configured for each day.

3. **Set the Alarm Actions Taken for Motion Detection**

Purpose:

You can specify the alarm type when an event is triggered.

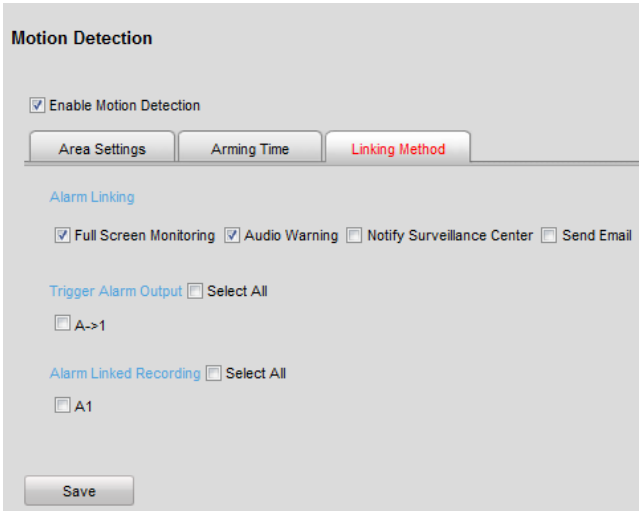


Figure 7.13 Motion Detection-Linking Method

Steps:

(1) Click the **Linking Method** tab to enter the setting interface.

(2) Select the alarming linkage method(s) including Full Screen Monitoring, Audio Warning, Notify Surveillance Center and Send Email.

- **Full Screen Monitoring**

When an alarm is triggered, the video image from the alarming channel configured for "full

screen monitoring" will be displayed in full screen.

- **Audio Warning**

Trigger an audible beep when an alarm is detected.

- **Notify Surveillance Center**

Send an exception or alarm signal to remote alarm host when an event occurs. The alarm host refers to the PC installed with Remote Client.

- **Send Email**

Send an email with alarm information to a user or users when an event occurs.

Note: To send the Email when an event occurs, you need to go to the network setting interface to set the related parameters. Refer to *Section6.3.4 Configuring Email Settings.*

(3) Select the channel you want to trigger an external alarm output when a motion detection event occurs.

Figure 7.14 Motion Detection-Trigger Alarm Output

Note: To trigger an external alarm output when an event occurs, you need to go to the Alarm Output Settings interface to set the related parameters.

1) Click **Remote Configuration> Alarm Settings> Alarm Output** to enter the Alarm Output Settings interface.

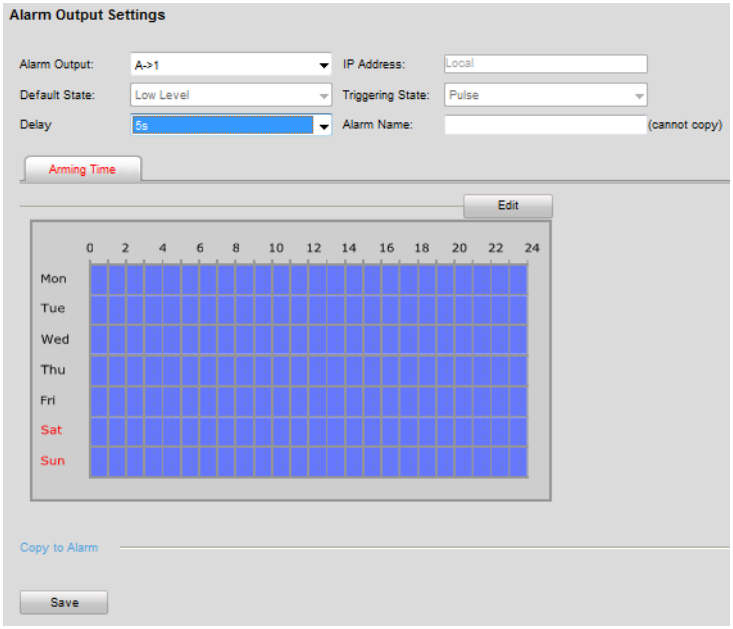


Figure 7.15 Motion Detection-Alarm Output Settings

2) Select one alarm output channel in the **Alarm Output** drop-down list.

3) The D**elay** time can be set to **5sec**, **10sec**, **30sec**, **1min**, **2min**, **5min, 10min** or **Manual**.

The **Delay** refers to the time duration that the alarm output remains in effect after alarm occurs.

Note: If you choose **Manual**, you need to manually disable the alarm output.

4) Click **Edit** to enter the **Edit Schedule Time** interface. The time schedule configuration is the same as the Setting of the Arming Schedule for Motion Detection. Refer to *Step 2* ***Set the Arming Schedule for Motion Detection*** in *Section 7.3.1 Configuring Motion Detection.*

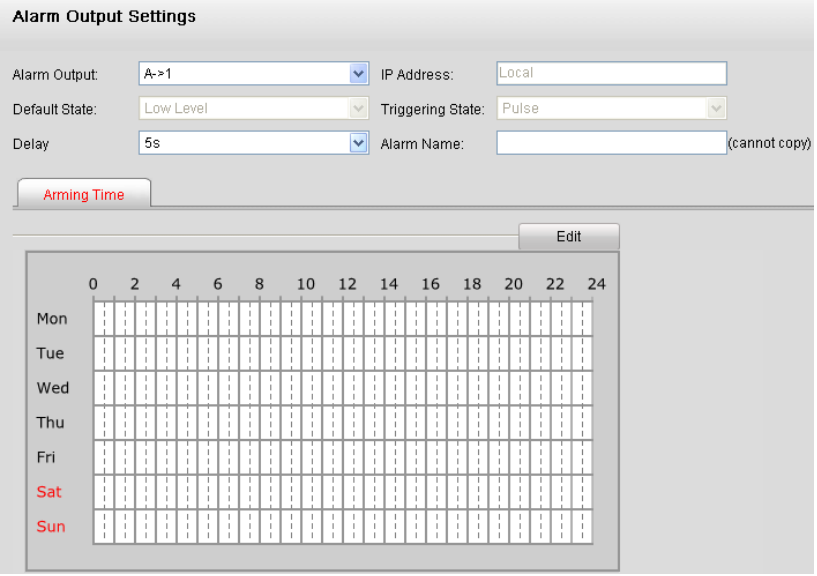


Figure 7.16 Motion Detection-Alarm Output Settings

5) Return to the Alarm Output Settings interface and click **Save** to save the settings.

(4) Select the channel you want to trigger recording when a motion detection event occurs.

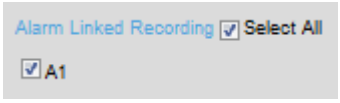


Figure 7.17 Motion Detection-Alarm Linked Recording

(5) Click **Save** to save the settings of linking method motion detection.

7.3.2 Configuring External Alarm Input

Steps:

1. Click **Remote Configuration> Alarm Settings> Alarm Input** to enter the Alarm Settings interface.
2. Choose the alarm input number and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed).

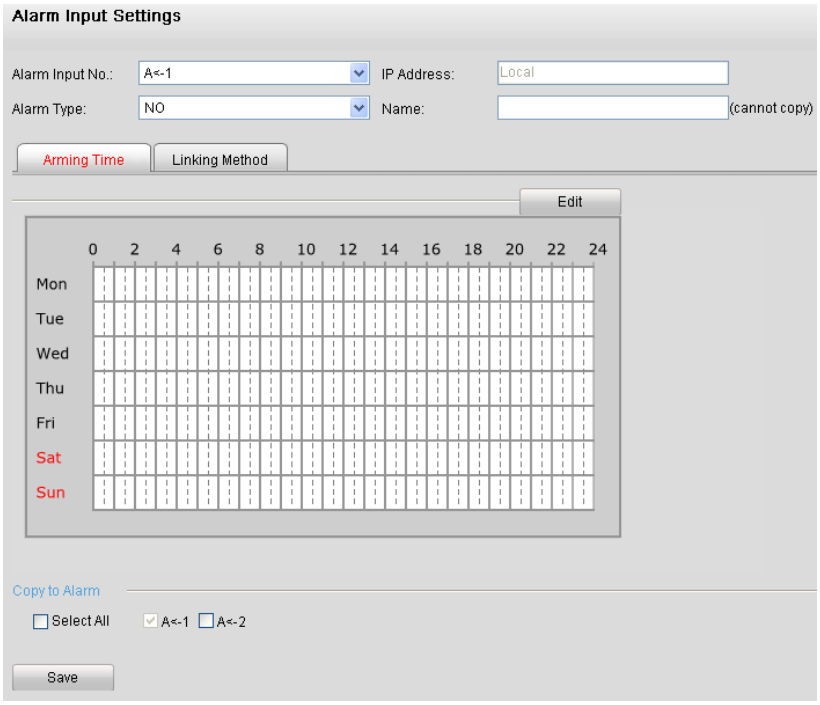


Figure 7.18 Alarm Input Settings-Arming Time

3. Set the arming schedule for the alarm input. Refer to *Step 2* ***Set the Arming Schedule for Motion Detection*** in *Section 7.3.1 Configuring Motion Detection.*
4. Click the **Linking Metho**d tab to set the actions taken for the alarm input. Refer to *Step 3* ***Set the Alarm Actions Taken for Motion Detection*** in *Section 7.3.1 Configuring Motion Detection*.
5. You can also choose the PTZ linking for the alarm input if your camera is installed with a pan/tilt unit.
   (1) Choose the PTZ Linking channel.
   (2) Check the relative checkbox to enable Preset Calling, Patrol Calling or Pattern Calling.

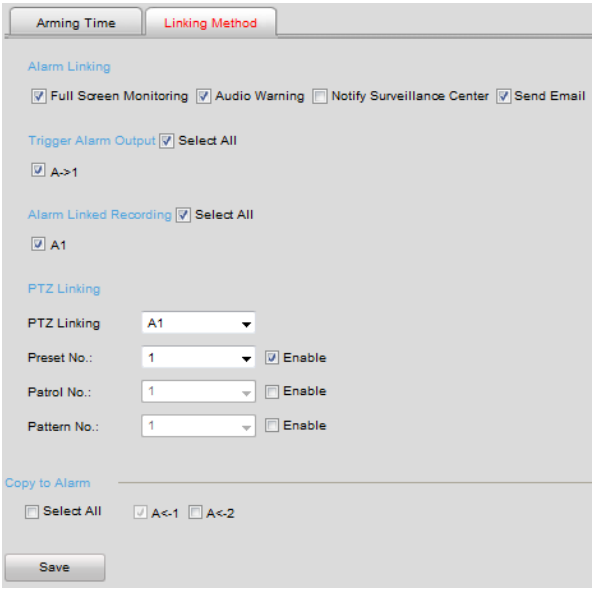


Figure 7.19 Alarm Input Settings-Linking Method

6. You can copy your settings to other alarm inputs.
7. Click **Save** to save the settings.

7.3.3 Configuring Video Loss Alarm

Steps:

1. Click **Remote Configuration> Camera Settings> Video Loss** to enter the video loss alarm setting interface.

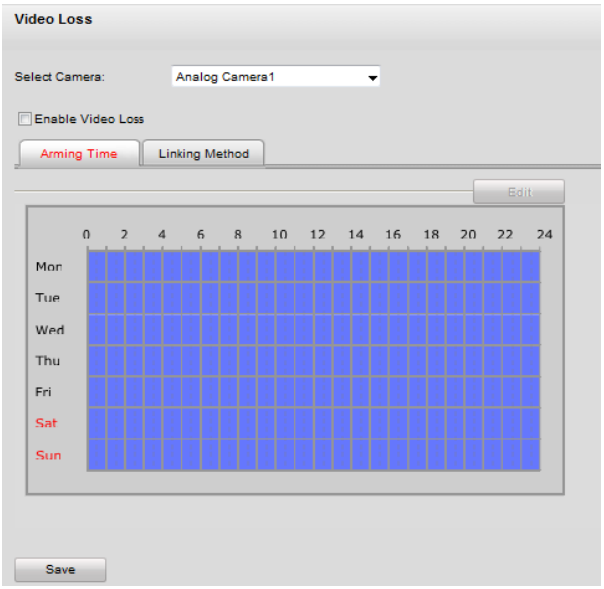


Figure 7.20 Video Loss Alarm Settings

2. Select the camera to configure the video loss alarm.
3. Check the checkbox of **Enable Video Loss**.
4. Click **Edit** to edit the arming schedule for video loss detection. The arming schedule configuration is the same as the Setting of the Arming Schedule for Motion Detection. Please refer to *Step 2 Set the Arming Schedule for Motion Detection* in *Section 7.3.1 Configuring Motion Detection.*
5. Click the **Linking Method** tab to set the actions taken for the video loss alarm. Please refer to *Step 3* **Set the Alarm Actions Taken for Motion Detection** in *Section 7.3.1 Configuring Motion Detection*.

7.3.4 Configuring Tamper-proof Alarm

Purpose:

If you enable this function, an alarm will be triggered when the image of camera is tampered with.

Steps:

1. Click **Remote Configuration> Camera Settings> Tamper-proof** to enter the Tamper-proof Settings interface.
2. Select the camera to configiure the tamper-proof detection alarm.

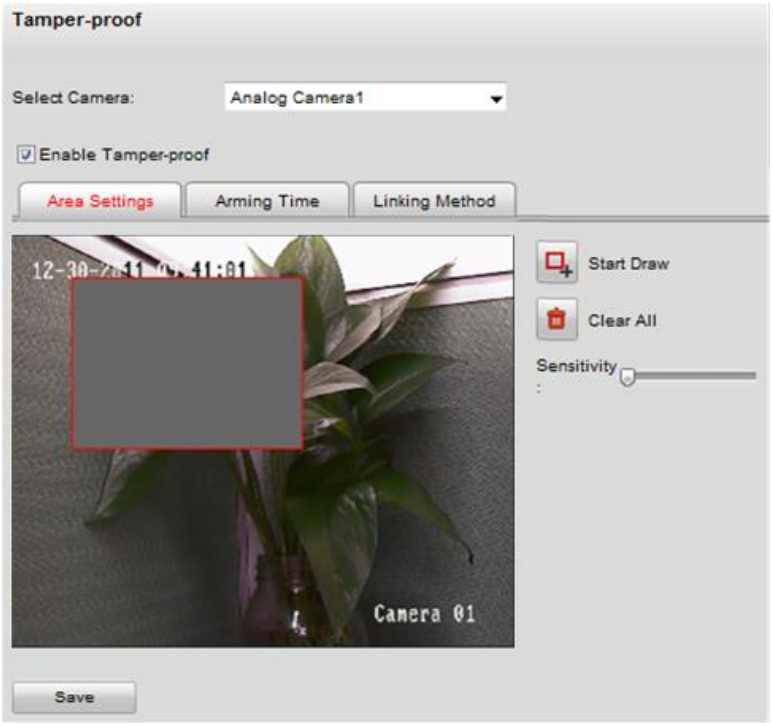


Figure 7.21 Tamper-proof Alarm Settings

3. Click checkbox of **Enable Tamper-proof**.
4. Set the tamper-Proof area. Please refer to *Step 1 Set the Motion Detection Area* in *Chapter 8.3.1.*
6. Click **Edit** to edit the arming schedule for tamper-proof. The arming schedule configuration is the same as the Setting of the Arming Schedule for Motion Detection. Please refer to *Step 2 Set the Arming Schedule for Motion Detection* in *Section 7.3.1 Configuring Motion Detection.*
7. Click the **Linking Method** tab to set the actions taken for the tamper-proof alarm. Please refer to *Step 3* **Set the Alarm Actions Taken for Motion Detection** in *Section 7.3.1 Configuring Motion Detection*.

7.3.5 Handling Exception

The exception type can be HDD full, HDD error, network disconnected, IP address conflict, illegal access, video standard mismatch, video signal exception, record/capture exception and video resolution mismatch.

Note: When the selected resolution under **Remote Configuration > Camera Settings >Video Settings** and the actual video input resolution are mismatched, the exception alarm will occur. Please refer to *Section 7.2 Configuring Video Settings.*

Steps:

1. Click **Remote Configuration> Exception** to enter the Exception Settings interface.
2. Check the checkbox to set the actions taken for the Exception alarm. Please refer to *Step 3* ***Set the Alarm Actions Taken for Motion Detection*** in *Section 7.3.1 Configuring Motion Detection*.

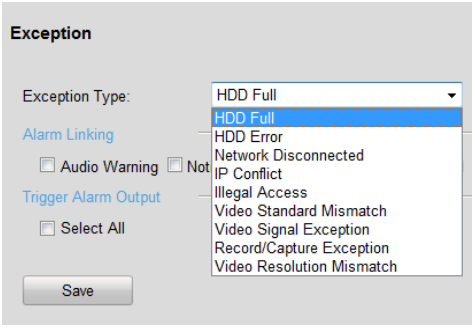


Figure 7.22 Handling Exceptions

3. Click **Save** to save the settings.

7.4 Configuring Privacy Mask

Purpose:

Privacy Mask enables you to cover certain areas on the video of the channel to prevent your privacy from live viewing and recording.

Steps:

1. Click **Configuration>Remote Configuration>Camera Settings>Privacy Mask** to enter the privacy mask settings interface.
2. Select the camera to configure privacy mask.
3. Check the checkbox of **Enable Privacy Mask** to enable this function.

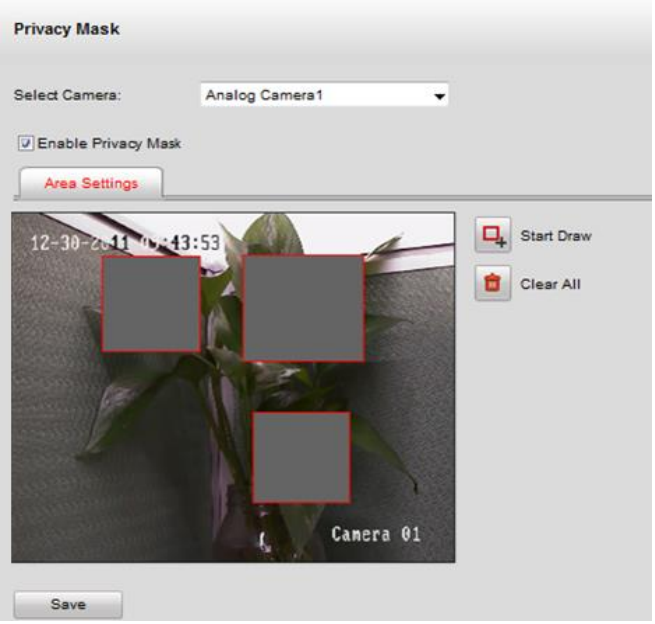


Figure 7.23 Privacy Mask Settings

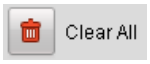
4. Click the

button.
5. Draw the mask area by clicking and dragging the mouse in the live video image.

Note: Up to 4 privacy mask areas can be configured.

6. When finishing the area setting, click the

button to finish drawing.

You can click the 

button to clear all of the areas you set without saving it.

7. Click **Save** to save the settings.

7.5 Configuring RS-232/485 Settings

7.5.1 RS-232 Settings

Purpose:

The RS-232 serial port can be used for the configuration by the serial port management tools.

Steps:

1. Click **Remote Configuration> Serial Port Settings> 232 Serial Port** to enter RS-232 port setting interface:

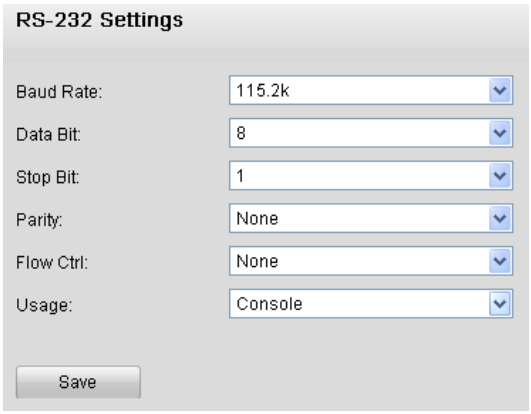


Figure 7.24 RS-232 Port Settings

Note: If you want to connect the camera by the RS-232 port, the parameters of the RS-232 should be exactly the same with the parameters you configured here.

2. Click **Save** to save the settings.

7.5.2 RS-485 Settings

Purpose:

The RS-485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

Steps:

1. Click **Remote Configuration> Serial Port Settings> 485 Serial Port** to enter RS-485 port setting interface:

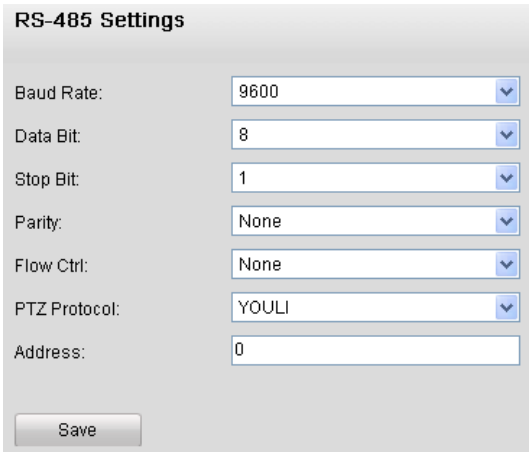


Figure 7.25 RS-485 Port Settings

2. Set the RS-485 parameters.

   By default, the Baud Rate is set as 9600, the Data Bit as 8, the Stop Bit as 1 and the Parity and Flow Control as None.

   Note: The Baud Rate, Address and PTZ Protocol parameters should be exactly the same as the parameters of the connected PTZ camera.

3. Click **Save** to save the settings.

Chapter 8 Managing User Accounts

Click **Remote Configuration**>**Remote Configuration**>**User Management** to enter the User Information interface:

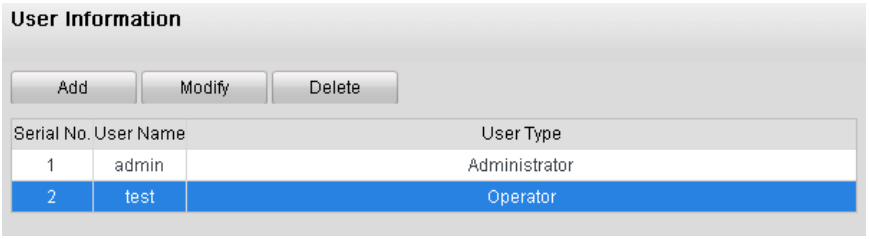


Figure 8.1 User Information Interface

The **admin** user is allowed to create normal users. And up to 31 users can be created.

8.1 Adding a User

Steps:

1. Click **Add** to enter the setting interface.
2. Input the **User Name** and **Password.**
3. Select the **User type** to **Operator** or **User.**

   The user type indicates the permissions you give to the user.

   - **Operator:** The *Operator* user level has permission of Local Log Search in Local Configuration, Remote Log Search and Two-way Audio in Remote Configuration and all operating permission in Camera Configuration.
   - **User:** The Guest user has permission of Local Log Search in Local Configuration, Remote Log Search in Remote Configuration and only has the local/remote playback in the Camera Configuration.

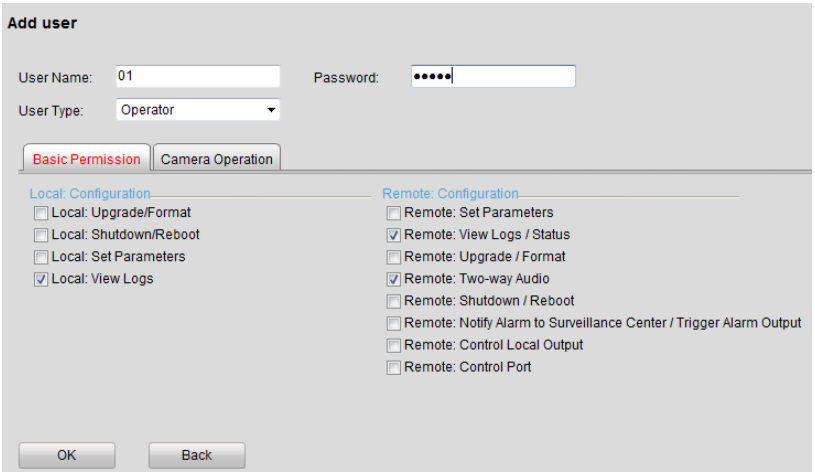


Figure 8.2 Add a User

4. Configure the user permission for the user, including the Basic Permission and Camera Operation.
5. Click **OK** to finish the user addition.

8.2 Modifying a User

Steps:

1. Select a user account from the list on the User Information interface to be modified.

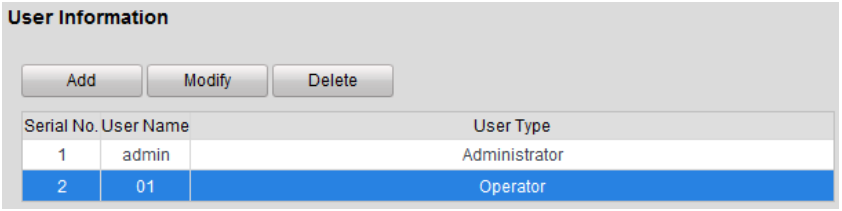


Figure 8.3 Select a User

2. Click **Modify** to enter the setting interface.

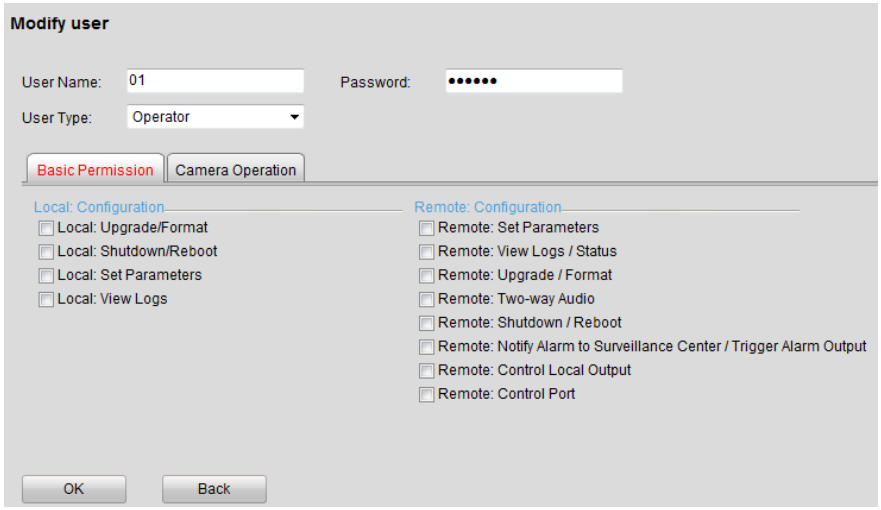


Figure 8.4 Modify a User

3. Modify the **User Name**, **Password** and then select **User type**.
4. Configure the user permission for the user, including the Basic Permission and Camera Operation.
5. Click **OK** to finish the user modification.

Note: You need the admin password to modify the admin user.

8.3 Deleting a User

Steps:

1. Select a user account from the list on the User Information interface to be deleted.
2. Click **Delete,** and the information box will pop up:

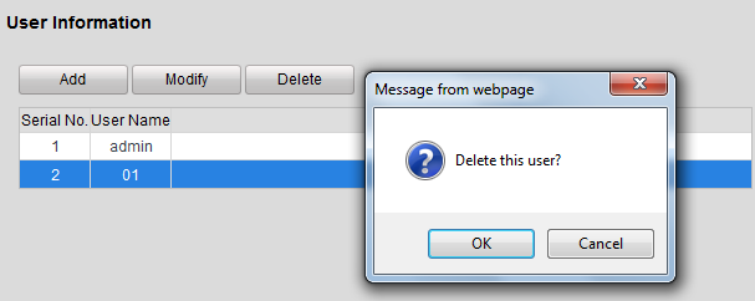


Figure 8.5 Delete a User

3. Click **OK** to delete the selected user account.

Chapter 9: Log Search and Maintenance

9.1 Log Search

Purpose

The operation, alarm, exception and information of the device can be stored in log files, which can be viewed and exported at any time.

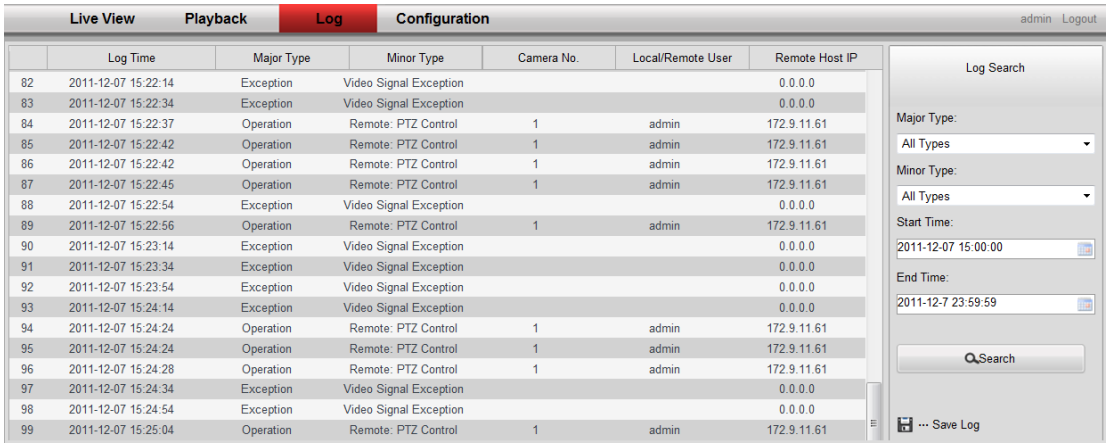
Before you start

The Log function can be realized only when the Encoder is connected with HDD (for VP-4HFI/HCI-SATA) or network disk. And make sure the HDD or network disk has been initialized for the first time to use. Please refer to *Section 6.3.5 Adding Network Disk* for details.

Steps:

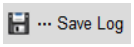
1. Click **Log** on the menu bar to enter the Log interface.
2. Set the log search conditions to refine your search, including the Major Type, Minor Type, Start Time and End Time.
3. Click the **Search** button to start searching log files.
4. The matched log files will be displayed on the list shown below.

   ***Note*:** Up to 100 log files can be displayed each time.



	Log Time	Major Type	Minor Type	Camera No.	Local/Remote User	Remote Host IP
82	2011-12-07 15:22:14	Exception	Video Signal Exception			0.0.0.0
83	2011-12-07 15:22:34	Exception	Video Signal Exception			0.0.0.0
84	2011-12-07 15:22:37	Operation	Remote: PTZ Control	1	admin	172.9.11.61
85	2011-12-07 15:22:42	Operation	Remote: PTZ Control	1	admin	172.9.11.61
86	2011-12-07 15:22:42	Operation	Remote: PTZ Control	1	admin	172.9.11.61
87	2011-12-07 15:22:45	Operation	Remote: PTZ Control	1	admin	172.9.11.61
88	2011-12-07 15:22:54	Exception	Video Signal Exception			0.0.0.0
89	2011-12-07 15:22:56	Operation	Remote: PTZ Control	1	admin	172.9.11.61
90	2011-12-07 15:23:14	Exception	Video Signal Exception			0.0.0.0
91	2011-12-07 15:23:34	Exception	Video Signal Exception			0.0.0.0
92	2011-12-07 15:23:54	Exception	Video Signal Exception			0.0.0.0
93	2011-12-07 15:24:14	Exception	Video Signal Exception			0.0.0.0
94	2011-12-07 15:24:24	Operation	Remote: PTZ Control	1	admin	172.9.11.61
95	2011-12-07 15:24:24	Operation	Remote: PTZ Control	1	admin	172.9.11.61
96	2011-12-07 15:24:28	Operation	Remote: PTZ Control	1	admin	172.9.11.61
97	2011-12-07 15:24:34	Exception	Video Signal Exception			0.0.0.0
98	2011-12-07 15:24:54	Exception	Video Signal Exception			0.0.0.0
99	2011-12-07 15:25:04	Operation	Remote: PTZ Control	1	admin	172.9.11.61

Figure 9.1 Log Search Interface

5. You can click the 

button to save the searched log files to local directory.

9.2 Viewing Device Information

Click **Remote Configuration > Device Parameters > Device Information** to enter the Device Information interface of the encoder:

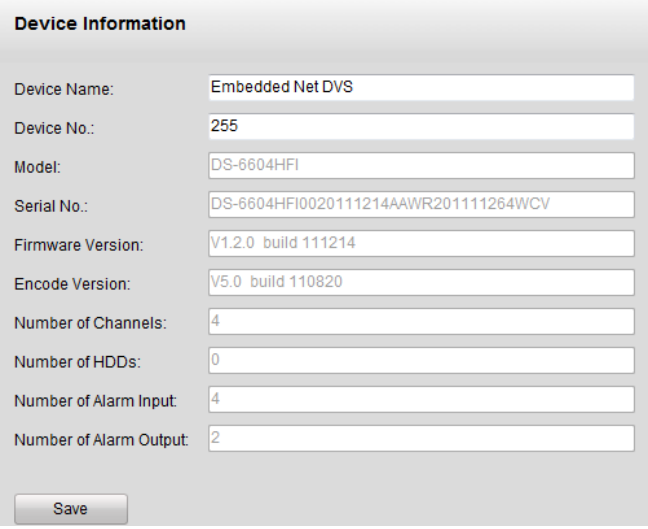


Figure 9.2 Device Information

You can edit the Device Name and Device No., and view the device information, including Model, Serial No., Firmware/Encode Version, Number of Channels, Number of HDDs, and Number of Alarm Input / Output.

9.2 Maintenance

Click **Remote Configuration >Maintenance** to enter the Maintenance interface of the encoder:

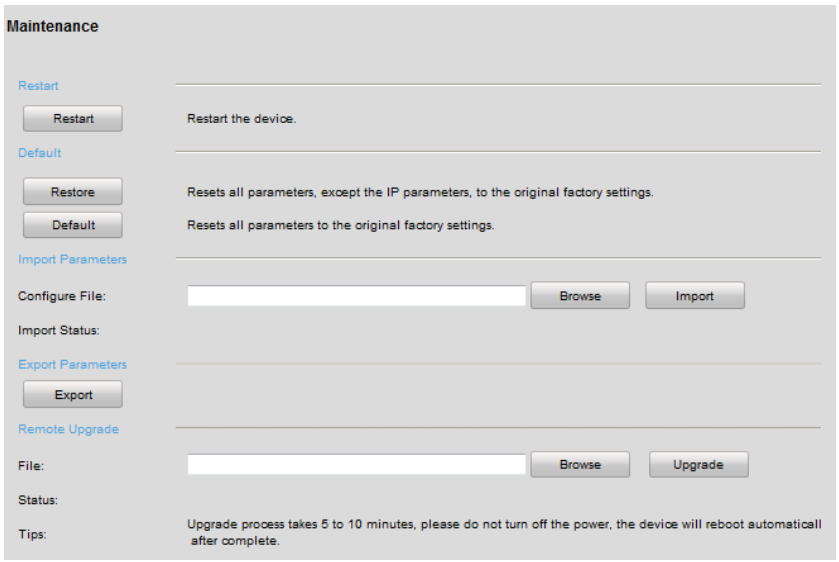


Figure 9.3 Maintenance Page

9.3.1 Restarting the Device

On the **Maintenance> Restart** interface, click **Restart** to enter the following dialog box:

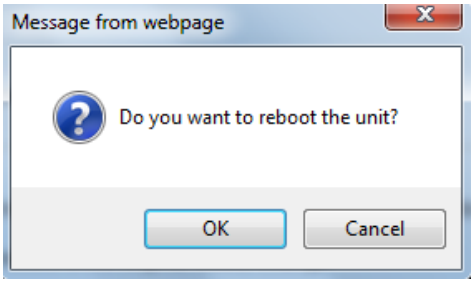


Figure 9.4 Restart the Device

Click **OK** to restart the device or **Cancel** to cancel the operation.

9.3.2 Restoring Default Settings

On the **Maintenance> Default** interface,, click **Restore or Default** to restore device parameters to the factory settings.

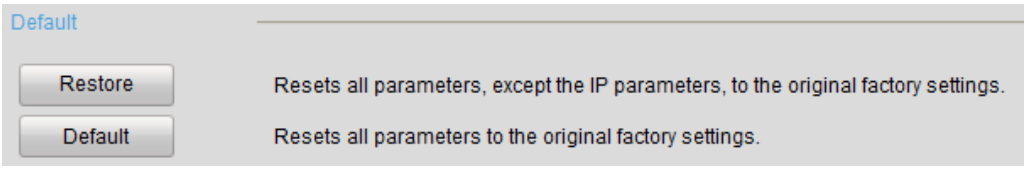

Default
Restore
Resets all parameters, except the IP parameters, to the original factory settings.
Default
Resets all parameters to the original factory settings.

Figure 12.5 Restore Default Settings

- By selecting the **Restore** button, the device restores the default settings for the parameters except the IP address, subnet mask, gateway and port.
- By selecting the **Default** button, the device restores the default settings for all parameters.

On the pop-up message box, click **OK** to restore and reboot the device to validate the settings.

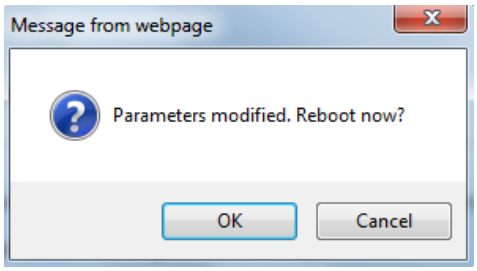


Figure 9.6 Pop-up Message Box

9.3.3 Importing/Exporting Parameters

The configuration files of the device can be exported to local device for backup; and the configuration files of one device can be imported to multiple device devices if they are to be configured with the same parameters.

- On the **Maintenance> Import Parameters** interface, click **Browse** to select the file from the selected backup device and then click the **Import** button to import a configuration file,

Note: After having finished the import of configuration files, the device will reboot automatically.

- On the **Maintenance> Export Parameters** interface, click the **Export** button to export configuration files to the selected local backup device.

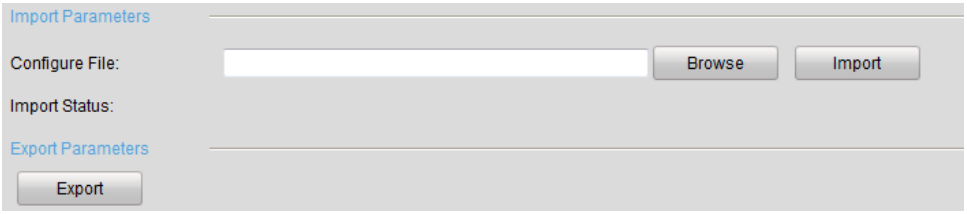


Figure 12.7 Import/Export Parameters

9.3.4 Upgrading the System

On the **Maintenance> Remote Upgrade** interface, click **Browse** to select the local update file and then click **Upgrade** to start remote upgrade.

Figure 9.8 Remote Upgrade

Chapter 10 Appendix

Appendix A FAQ

- **Why can't I ping the VP-4?**

  Please refer to Chapter 3 to configure the device's IP being in the same segment as your PC, and check the cable and switch.

- **If the transparent channel has been set, why is the encoder still not receiving data?**

  1. Check if RS-232 has been set as transparent channel first.
  2. Check the connection of encoder.

- **Why can't I control the connected PTZ camera or speed dome through the VP-4?**

  1. Check the RS-485 connection of the device with the PTZ camera or dome.
  2. Check whether the PTZ address, protocol and baud rate of the device are set to be the same with the connected camera or speed dome.

- **Why can't I view the video image through IE browser?**

  1. Check the network connection.
  2. Check the user name and password of DVS are entered correctly.
  3. Check the port of DVS is entered correctly.

Appendix B Glossary

Dual Stream

Dual stream refers to that one channel of video stream can be divided into double independent output streams through the video encoder. Shown as below:

The resolution, frame rate, bitrate and other parameters of the output stream are independently programmable. The two streams generated may meet different application demands, e.g., one stream is used for HDD storage, and the other for transmission via Internet.

Transparent Channel

The transparent channel indicates the channel used for transmitting data, and through which the data transmitted receives no handling and thus retains no change. By remotely connecting the keyboard with the decoder, the transparent channel can be established to realize control of dome or Pan/Tilt unit connected to remote encoder.

Resolution

The type of resolution can be divided into the display resolution, image resolution and pixel resolution.

The display resolution refers to the maximum display zone on the screen in certain display mode, measured in horizontal and vertical pixel.

The image resolution describes the detail a digital image holds, measured in horizontal and vertical pixel as well.

In case the image resolution is higher than the display resolution, proportion of the image will not be displayed on the screen.

The pixel resolution indicates the ratio of the pixel width and length. Different pixel width/length ratio will result in different shape of image.

Generally the image resolution is applied to the digital surveillance:

PAL: QCIF (176*144), CIF(352*288), 2CIF(704*288), DCIF(528*384), 4CIF(704*576).

NTSC: QCIF (176*120), CIF(352*240), 2CIF(704*240), DCIF(528*320), 4CIF(704*480).

The display resolution is usually applied to VGA monitor:

640*480, 800*600, 1024*768, etc.

Streaming Server

The streaming server refers to a dedicated computer system or server which runs the corresponding streaming media software to provide the delivery of data. It is generally applied to the delivery of the same massive data, which may greatly reduce the load of the host as well as save internet resources.